Semi-Blind Secure Watermarking based on integration of AES and ECC in DCT Domain

VINEET MEHAN

Copyright protection and integrity of digital images have become one of the vital issues in crucial watermark applications like Cheque Truncation System (CTS), Patient record management system and e-document verification etc. This paper illustrates an integrated watermarking and encryption technique to safeguard copyright of images and to offer security to the watermarked image contents. Watermarking technique based on combination of Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) in Discrete Cosine Transform (DCT) is proposed in this work. 25 sets of watermark are classified for embedding owner details with a size variation of 256–3328 bits. Watermark sequence and the secret keys are the prime requisite in the semi-blind approach for the extraction purpose. Peak Signal to Noise Ratio (PSNR), Structural similarity index measure (SSIM), Correlation Coefficient (CC), Net Pixel Change Rate (NPCR) and Entropy are specified in the objective function to identify noise, structural match, association, variation and imperceptibility factors. The experimental results display that the projected watermarking scheme offers better quantitative parameter outcomes in comparison with previous related techniques.

Manuscript received July 5, 2017; revised January 26, 2018; released for publication January 30, 2018.

Refereeing of this contribution was handled by Alexander Toet.

Author's address: Maharaja Agrasen Institute of Technology, Maharaja Agrasen University, Baddi 174103, H.P., India (E-mail: mehanvineet@gmail.com).

1557-6418/18/$17.00

1. INTRODUCTION

Unauthorized distribution and protection of intellectual digital property raised the need of Watermarking techniques. Watermarking has emerged as a prominent practice in the last decade. Digital data subversion has generated a number of concerns around digital authentication, reliability and copyright defence.

Unrestricted and easy transmission of information is also one of its greatest weaknesses, leading to the copying and outright theft of information, particularly images. Increase in use of digital images brings about the necessity for individuals to safeguard their digital assets. Given the motivation to protect intellectual property by ownership definition and security concerns; a watermarking with AES and ECC for digital images has been suggested as a form of secure watermarking scheme for images.

An expert crafts a digital image with due exertions along with a price. When illegitimate imitation of the image is found on the web, then the proprietorship correlated with the image is to be determined. Due to this delinquent, a practice called watermarking was announced to defend the copyright of digital images with its creative holder. The system of implanting data into digital image is labelled as digital watermarking [1]. Data to be injected into the image is called a watermark. Inserted watermark can be mined in future for the tenacity of proof of identity and verification [2]. Amendment triggered by entrenching the watermark is controlled to preserve visual resemblance amongst the host and the watermarked image [3]. The watermarking scheme can be represented symbolically by

$$I_w = E(I_o, W) \tag{1}$$

(1) where I_o, W and I_w denote the original image, the watermark containing the owner information, and the watermarked image, respectively. For watermark recognition, a perceiving function P is used. This operation is represented by

$$W' = P(I_w, I_0) \tag{2}$$

The extracted watermark sequence W' is then compared with the original W using a correlation measure θ given as

$$\theta(W, W') = \begin{cases} 1, & \text{if } t > \gamma \\ 0, & \text{otherwise} \end{cases} \tag{3}$$

where t is the value of the correlation and y' is a positive threshold. One bit watermarking is aimed to identify the existence or the lack of the watermark in the discernable object. Multiple bit watermarking includes a message (M) with n-bit long stream

$$M = \{0,1\}^n \tag{4}$$

such that ($m = m_1, m_2, \ldots m_n$, with $n = |m|$)

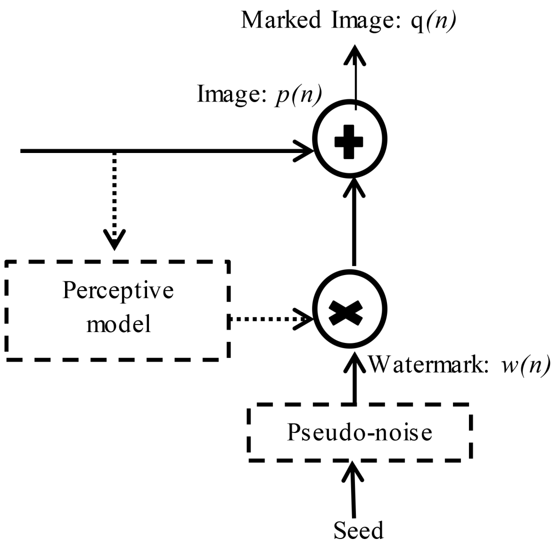

Fig. 1. Perceptible Watermarking Model

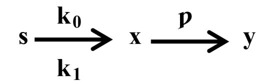

Fig. 2. Robust watermark detection

TABLE 1.
Comparative Analysis of DFT, DWT and DCT.

S. No.	Parameter	DFT	DWT	DCT
1.	Computational Complexity	High	High	Low
2.	Coefficients	Real and Imaginary	Real and Imaginary	Real
3.	Energy Compaction Property	Low	Moderate	High
4.	Block Artifacts	More	Less	Less
5.	Periodicity	More Discontinuous	Discontinuous	Less Discontinuous

Watermarking is categorized into subsequent two classes as per visual insight [4]: Perceptible watermarking and Imperceptible watermarking. Perceptible watermarks work is of assertion of proprietorship and origin [5]. Figure 1 shows the perceptible watermarking model. Observable watermarks decrease the value of an image for an offender devoid of dropping its value for genuine legal tenacities [6]. Imperceptible watermarks are also termed as invisible watermarks [7], as in this the watermarks are not apparent on the image. Watermarks are implanted in the digital image such that visible modification amongst the cover and watermarked image is not perceived [8].

Imperceptible watermarking is categorized as: Fragile watermarking and Robust watermarking. Fragile watermarking is castoff for image certification [9] to attest that acknowledged image was not altered in the course of communication. Even a minor alteration of the image, eliminates the implanted watermark. Fragile watermarking turn into semi-fragile watermarking if a definite boundary is fixed for amendment [10]. Robust watermarking is castoff for safeguarding copyright [11]. In robust watermarking, the inserted evidence is not aloof when the image is altered. Even an enormous extent of alteration does not eradicate the watermark that has been implanted [12].

Figure 2 shows robust watermark detection where s is a vector signal such that $s = (s_1, s_2, \ldots, s_n) \in S^n$ of n-dimensional multimedia host signal; k is an integer from an index set $K = \{1, 2, \ldots, k\}$ where K is total number of messages; x is an authenticated signal such that $x \in S^n$ without hosting perceptible visual distortion; p is a probability density function; and y is the channel output.

Watermarking is classified into two groups [13] depending upon the processing realm : Spatial domain watermarking and Frequency domain watermarking Spatial domain watermarking changes the content of the image pixels unswervingly based on the watermark that has to be implanted [14]. The key benefit of this system is reduced computational complexity and less time [15]. Frequency domain system transforms an image from spatial domain to frequency domain. Watermark is injected into the frequency coefficients. Inverse transform is then smeared to transmute it back into spatial domain. Frequency domain practice is more robust than spatial domain system. Commonly used frequency domain transforms are Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) [16–22]. DCT has been widely used for watermarking applications among all the transforms due to low computational complexity, less block artifacts and high energy compaction property as shown in Table 1.

2. LITERATURE SURVEY

Potdar et al. in 2005 [23] recommended three diverse types of watermarking on the basis of mining prerequisite of the watermark. These include: Non-blind watermarking, semi-blind watermarking and blind watermarking [24]. In non-blind watermarking original image is essential for the abstraction of the watermark. In semi-blind watermarking, only the watermark signal is vital for the removal of the watermark. In blind watermarking no other evidence is required apart from the watermarked image. In our proposed work an efficient semi-blind watermarking scheme is perceived by retrieving the watermarks from the watermarked image. In semi-blind approach only the watermark sequence and the secret keys are needed for the extraction purpose. As in most of the watermark applications original image is not available to the detector, thus the approach exhibits to be more advantageous than the non-blind approach. A semi blind watermarking notation is given as

$$D_d : \bar{I} \times I \times W \square \acute{I} \times \acute{W} \cup \{\perp\} \text{ and}$$
$$X_x : \bar{I} \times I \times \acute{W} \square \acute{M} \times \acute{K} \cup \{\perp\} \quad (5)$$

where D is detection function; X is extraction function and W is a watermark.

A combination of robust and fragile watermarking scheme is designed by Zhang et al. in 2008 [25]. In the robust process watermark is encrypted using AES. DCT is applied to the blue component of the image for embedding watermark. In the fragile process red component of the image is hashed using SHA-256 and then encrypted using ECC key and finally embedded using LSB technique. Our paper used AES with 256 bit key using frequency coefficients rather than in spatial domain. Key generated in our approach is using ECDHP which is immune to attacks and can be used for copyright protection, image integrity certification and identity authentication.

A multipurpose image watermarking with public key cryptography is proposed by Ding et al. in 2008 [26]. A blend of copyright protection is done with content authentication using error correcting codes. In our proposed approach watermarks are implanted into separate DCT coefficients as per image block size. To build up security, the watermarking process makes use of the ECC, ECDHP and AES instead of RSA algorithm as is used in this paper.

3. WATERMARKING APPLICATIONS OF PROPOSED MODEL

Watermarking finds enormous interesting applications in the field of multimedia, image processing and e-commerce etc. Some of the key applications associated with the proposed work are given as:

3.1. Cheque Truncation System

Cheque Truncation System (CTS) is a practice of averting physical crusade of cheque by switching it with a digital image, with an intention for secure and quicker clearance [27]. Watermarking can be applied in the domain of cheque truncation where the cover image is a scanned cheque image. Watermarks to be implanted into the image may encompass user and cheque details. Embedded watermark can be detached later for the purpose of credentials and validation to be exploited for making transactions.

Progression in technology leads to development of novel algorithms and standards by substituting with previous security standards. Standards must take account of aspects like authentication and dependability with the sharing of images in CTS for making transactions. The projected method applies new principles and processes to CTS which tends to be highly consistent and targets at achieving the standardized practice. Watermarking methodology and secure algorithms assistance to offer data reliability, security, and certification solutions to CTS. Watermarking has been proposed as a standard system to solve the anomalies concomitant with CTS. Comparative Analysis of Reserve Bank of India (RBI) based CTS with our proposed approach is shown in Table 2.

TABLE 2.
Comparative Analysis of RBI based CTS [26] with our proposed approach.

Parameter	RBI-CTS	Proposed CTS
Key Generation	DH	ECDHP
Asymmetric Encryption	RSA	ECC
Symmetric Encryption	Triple DES	AES
Image Specification	Gray Scale	Color Image

The proposed effort will corroborate advantageous for the CTS systems being activated in developing countries and will also aid the developed countries to weigh up their prevailing CTS procedures.

3.2. Copyright Protection and Owner Identification of Digital Images

Digital watermarking system allows an individual to add copyright notices and other verification messages to image signals. Such a message is a group of bits describing information pertaining to the owner of the image. The messages can be easily detached by cropping the image part that has the identification. Digital watermarking helps to overcome this problem by embedding the watermark in the form of bits that forms an integral part of the content. In the case of dispute over ownership of the host data, embedded watermark can be used as a proof to identify the true owner of the host data. Image selling portals like imagesbazaar.com carry over one million digital images of Indian visuals. Images at this portal cost substantially depending upon the theme and the style. Proposed technique helps in securing the digital image present online by inserting copyright details.

3.3. Patient Record Management System

Digital watermarking is useful in the e-health environment for tele-consulation and tele-diagnosis purpose [28] Medical images encompass diagnostic information which can be used for timely detection of the diseases. It is useful to safeguard patient data, content certification and medical image reliability. Images are watermarked to prove the integrity by confirming that the image was not altered by illicit person [30]. Watermarking is also applied to determine the authenticity by confirming that the image belongs to the right patient and exact source.

The proposed approach can play an effective role in the management of patient's record. Using this technique vital information related to patient like name, patient id, disease name and patient's photo can be embedded in the medical image. This will prevent the error of mismatching records of patients.

3.4. Certification of Electronic Passport

Certification is a substantial staple for documents, such as electronic passports. Fortification of validity in passport raised the necessity for the implementation of electronic passport [31]. Electronic Passport is alike to the regular passport with addition of a slight integrated circuit to store digital image [32]. The proposed method permits secure and imperceptible storing of passport details which may include passport number, name of passport owner and other important passport credentials within a digital image. Any variation done to the stored image will result in authentication failure which can be easily identified using the proposed approach.

Usual exercise of programmed passport authorization contests the image existent in the chip with the appearance of the passport holder [33]. The scheme deportment limits when the modifications are not perceived in the image. Prevailing method does not observe the swapping of the passport image with an alternative image. The foremost facet of this verification method is to introduce an orientation between passport's particulars and implanted image insides. Application of digital signature tools legalizes the precision of the evidence retained in the image. It defends passport's genuineness opposing to fraud and security crevices.

The exploration effort proposed by this research work can be used for automatic verification mechanism of passport to be used for immigration clearance system installed at airports. The proposed scheme can also be applied to other important certification documents which include driving licence, identification cards, institute certificates, university degrees and official government documents.

4. SECURE WATERMARKING COMPONENTS

Secure watermarking integrates ECC, ECDHP and AES properties to solve key distribution problem and security concerns for watermarking.

4.1. ECC based Encoding

Elliptic curve cryptography is an asymmetric key cryptosystem which relies on the computational hard discrete logarithm of an elliptic curve [34]. ECC techniques do not perform encryption and decryption of actual data rather they encrypt and decrypt points on the curve. Encoding translates a message into points defined by the elliptic curve, while decoding translates the points back to the original message [35].

ECC operations use multiplication operations instead of exponentiation operations. This makes ECC much faster than other public key cryptosystem like RSA. The security level specified by RSA can be delivered by reduced key size of ECC. For example, the 1024 bit security strength of a RSA can be obtained by only 163 bit security strength of ECC [36]. In the proposed work ECC's small key size, high security and reduced computational complexity characteristics are integrated with digital watermarking for improved ownership protection.

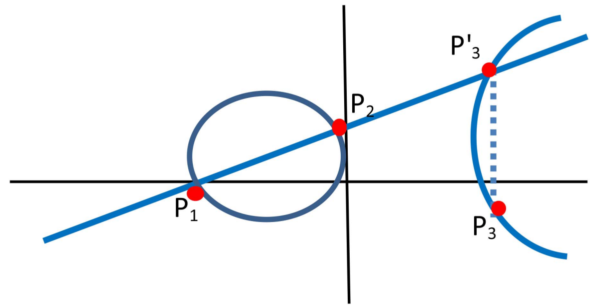

Fig. 3. Adding points such that $P_1 \neq P_2$

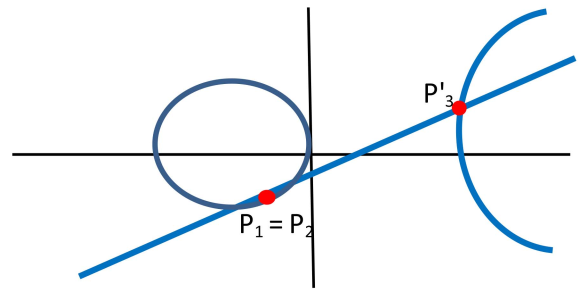

Fig. 4. Adding points such that $P_1 = P_2$

Elliptic curves are customarily signified using Weierstrass [37–39] devising in the most common form. An elliptic curve E_c on a prime field F_p is specified as

$$E_c(F_p) : y^2 = x^3 + ax + b \qquad (p > 3) \tag{6}$$

where $a, b \in F_p$ and $\Delta = -16(4a^3 + 27b^2) \neq 0$. Different choice of a and b gives different elliptic curves. A true condition of Discriminant (Δ) forms Group Law [40–44]. There can be three cases in this situation.

Case 1: To add two separate points P_1 and P_2 such that $P_1 \neq P_2$. For an equation $y^2 = x^3 - x$ the elliptic curve is shown in Figure 3.

Step 1. Join the two points i.e. P_1 and P_2 on an elliptic curve.

Step 2. The line will also intersect the elliptic curve at P_3'.

Step 3. Reflect the line to get point P_3.

Case 2: To add two points P_1 and P_2 such that $P_1 = P_2$. For the same equation $y^2 = x^3 - x$ the elliptic curve is shown in Figure 4.

Step 1. Find the tangent line to pint P_1 on an elliptic curve.

Step 2. Find the second point of intersection i.e. P_3'

Step 3. Reflect P_3 to get point P_3'.

Case 3: In case of parallel lines it is assumed that the line from P_1 to P_2 will intersect the curve at ∞. In this case the elliptic curve is shown in Figure 5.

In order to find the coordinates of third point using Group Law the line equation (7) is computed with

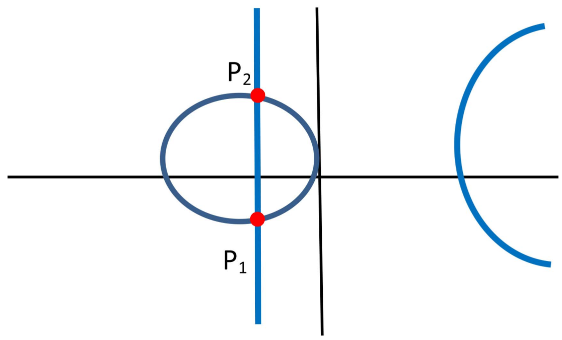

Fig. 5. Adding vertical lines

elliptic curve equation.

$$y = mx + b \tag{7}$$

Let $m = \lambda$ and $b = \beta$ be substituted in equation (7) such that

$$y = (\lambda x + \beta) \tag{8}$$

$$y^2 = (\lambda x + \beta)^2 \tag{9}$$

$$(\lambda x + \beta)^2 = x^3 + ax + b$$

$$\lambda^2 x^2 + \beta^2 + 2\lambda x\beta = x^3 + ax + b$$

$$x^3 - \lambda^2 x^2 - 2\lambda x\beta + ax + b - \beta^2 = 0 \tag{10}$$

For a cubic equation (5) let x_1, x_2 and x_3 are the three roots such that

$$x_1 + x_2 + x_3 = \lambda^2$$

$$x_3 = \lambda^2 - x_1 - x_2 \tag{11}$$

Using point slope form between points (x_1, y_1) and (x_3, y_3)

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

$$y_3 = y_1 + \lambda(x_2 - x_1) \tag{12}$$

Our contribution in this work is to apply logical non-linear ECC curve points to safeguard watermark insertion against active content identification attacks. The proposed algorithm performs selective encoding on the transform coefficients. Encoding converts owner details into points defined by the elliptic curve in order to be suitable for encryption. Decoding converts the points into the original message at the time of retrieval.

4.2. Key generation with ECDHP

Traditional digital rights management (DRM) schemes involve a twofold structure consisting of only owner and the buyer. With the ascendable rise in digital industry multi-level distributors and sub-distributors are needed to support and circulate the digital content [45]. A native distributor can identify the possibly unfamiliar marketplace to the owner and make strategies as per the requirement of the trade. But at the same time, a selfish distributor can pass on the digital content to other consumers without the consent of the owner. ECDHP solves this content packaging mechanism by generating key among all the owners, distributors and sub-distributors. ECDHP is a deviation smeared to Diffie Hellman technique through ECC [46]. The method allows members without any former consociate, to reciprocally generate a shared key above a susceptible network [47]. The content packaging system is handled without the need of a license granting authority [48]. The key is used in encrypting the credentials of all the persons involved in the chain. The owner then passes the watermarked content containing the embedded encrypted credentials to the next level for distribution. Key generation (K_G) by ECDHP prevents the illegal circulation of digital content among multiple owners, distributors and sub-distributors.

NIST based elliptic curves are challenging to solve as the discrete log problem is strong. Key created by the system can be castoff by cryptographic organizations to defend the legitimacy and cover up of the information [49]. Trustworthy heralds can tangibly distribute the secret key, but as the reckoning of key exchange upsurges, the power involved in the distribution of keys grows quickly. Programmed key establishing arrangement based on ECDHP assistances in the conservation of the cryptographic schemes applied in current dominions [50]. The procedure is appropriate to covenant with exclusivity, authorization, key agreement and accelerative concealment.

Key generation using ECDHP involves:

1. A_l and B_b agree publicly on elliptic curve (E_p) over a large finite field.
2. A_l and B_b each privately choose large random integer as secret key A_k and B_k.
3. Using elliptic curve point addition, A_l computes $(A_k G)$ on E_p and sends it to B_b.
4. Similarly, B_b computes $(B_k G)$ on E_p and sends it to A_l.
5. Both A_l and B_b can now compute the point $(A_k B_k G)$.
6. Shared secret key computed by both A_l and B_b is the same.

ECDHP forms efficient arithmetic with shorter key length. ECC provides enhanced security based on discrete logarithm problem. NIST prime curve is computationally efficient as it significantly reduces the total number of multiplies in an exponentiation. To protect a 256 bit symmetric key, RSA algorithm would require 15360 bit key size which is approximately 30 times greater than the size of elliptic curve with 521 bits.

4.3. Secure Watermark Encryption with AES in DCT Domain

AES is a symmetric block cipher algorithm. It uses iterated block cipher, supporting a static length block

TABLE 3.
AES algorithm parameters.

Algorithm	Key Length (words)	Block Size (words)	Number of Rounds
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

TABLE 4.
AES with ECC prime fields.

Symmetric Length	Algorithm	Prime Field	Binary Field
80	SKIPJACK	$\|p\| = 192$	$m = 163$
112	Triple-DES	$\|p\| = 224$	$m = 233$
128	AES Small	$\|p\| = 256$	$m = 283$
192	AES Med.	$\|p\| = 384$	$m = 409$
256	AES Large	$\|p\| = 521$	$m = 571$

of 128 bits [51, 52]. The AES algorithm primarily comprises of three phases: round change, turns and key expand. Each round conversion includes non-linear layer, linear mixture layer and add round key layer. AES algorithm properties are depicted in Table 3. Three key sizes of 128 bits, 192 bits and 256 bits specify different number of repetitions of transformation rounds.

Watermark security is safeguarded by encrypting owner details by means of AES with 256 bits key. Encrypted owner details are generated in multiple of 128 bits as per the block size specification of AES. Encrypted watermark is then implanted into the digital image. AES algorithm delivers watermark security as only a legitimate owner can retrieve and decrypt the inserted stuffing. AES is the preeminent recognized symmetric algorithm for encrypting information, but it suffers from the delinquent of key distribution [53–56]. The key distribution concern is elucidated using ECC by using ECDHP. A hybrid encryption algorithm of AES and ECDHP ensures the content security in digital watermarking. AES provide fast computing speed and encrypts lengthy data while ECDHP handles the key management issues. The projected scheme inhibits the confidentiality of owner data by conjoining encryption with watermarking. Table 4 gives the sizes of the various underlying fields. $\|p\|$ is the length of the binary expansion of the integer p.

Encrypted details are embedded in digital image using the DCT methodology. Only an authenticated user with secret key can retrieve the inserted watermarks from the specified positions within the watermarked image. DCT transforms the image from spatial domain to transform domain [57]. 2-D DCT of an $N \times N$ real signal matrix $f(x, y)$ $(x, y = 0, 1, 2, \ldots, N-1)$ is defined as

$$C(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{\pi(2x+1)u}{2N}\right] \times \cos\left[\frac{\pi(2y+1)v}{2N}\right] \tag{13}$$

$$\alpha(u)\alpha(v) = \begin{cases} \sqrt{\frac{1}{N}} & u = 0,\ v = 0 \\ \sqrt{\frac{2}{N}} & u \neq 0,\ v \neq 0 \end{cases} \tag{14}$$

where

$C(u, v)$: DCT coefficient at frequency (u, v)

$f(x, y)$: Original image pixel at location (x, y)

$x, y = 0, 1, 2, \ldots, N-1$

$u, v = 0, 1, 2, \ldots, N-1$

$\alpha(u)$ and $\alpha(v)$ are the scale factors needed to make DCT orthogonal

2-D inverse DCT of $N \times N$ image matrix is defined by the equation (10) [58] as shown below:

$$f(x,y) = \sum_{u=0}^{N-1}\sum_{v=0}^{N-1} \alpha(u)\alpha(v)\cos\left[\frac{\pi(2x+1)u}{2N}\right] \times \cos\left[\frac{\pi(2y+1)v}{2N}\right] \tag{15}$$

Matrix and image data define the necessary coefficients for implanting the watermark content. Mid frequency coefficients at $[2, 0]$ position are altered within each 4×4 quantised block. Separability [59] and Symmetry [60] characteristics of DCT are exploited to create a 4-point DCT in matrix form. If two 1D elementary functions are same, the transform is said to be symmetric.

$$A_{k,l}(m,n) = a_k(m)b_l(n) = a_k(m)a_l(n) \tag{16}$$

This expression allows a notation in terms of the analysis matrix A associated with the 1D Transform

$$Y = A * XA^H \tag{17}$$

where,

$$X = \begin{pmatrix} x(0,0) & \cdots & x(0,n) & \cdots & x(0,N-1) \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ x(m,0) & \cdots & x(m,n) & \cdots & x(m,N-1) \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ x(M-1,0) & \cdots & x(M-1,n) & \cdots & x(M-1,N-1) \end{pmatrix} \tag{18}$$

and

$$Y = \begin{pmatrix} y(0,0) & \cdots & y(0,n) & \cdots & y(0,N-1) \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ y(m,0) & \cdots & y(m,n) & \cdots & y(m,N-1) \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ y(M-1,0) & \cdots & y(M-1,n) & \cdots & y(M-1,N-1) \end{pmatrix} \tag{19}$$

TABLE 5.
Owner watermarks embedded in Q1.

Label	W. Content	W. Size (in bits)
W1	OID1	256
W2	W1 + ON1	384
W3	W2 + OHN1	512
W4	W3 + OSE1	640
W5	W4 + OC1	768
W6	W5 + OST1	896
W7	W6 + OMN1	1024
W8	W7 + OEM1	1152
W9	W8 + OID2	1280
W10	W9 + ON2	1408
W11	W10 + OHN2	1536
W12	W11 + OSE2	1664
W13	W12 + OC2	1792
W14	W13 + OST2	1920
W15	W14 + OMN2	2048
W16	W15 + OEM2	2176
W17	W16 + OID3	2304
W18	W17 + ON3	2432
W19	W18 + OHN3	2560
W20	W19 + OSE3	2688
W21	W20 + OC3	2816
W22	W21 + OST3	2944
W23	W22 + OCY3	3072
W24	W23 + OMN3	3200
W25	W24 + OEM3	3328

2-D DCT, configuration and disintegration are separable processes, consequently resizing of images can be consummate by applying 1-D operations successively in horizontal and vertical directions. Our resizing method with 1-D sequence includes a factor of S/T where S and T are relatively large prime numbers greater than 1. A total of U successive N-point DCT blocks are prerequisite. Each DCT block is zero padded to a size of SN and then decomposed into SN-point DCT blocks. Consequently, T disintegrated N-point DCT blocks are collected into a single TN-point DCT block. Each composed TN-point DCT block is then trimmed to a size of N.

Integration of AES with RSA to safeguard the watermark confidentiality consequences in intake of large key size grounded on integer factorization. Computationally proficient key exchange contrivance built on ECC can substitute this security constraint with smaller key size. AES is the finest recognized symmetric key cryptographic algorithm for encrypting information. It guarantees comprehensive safekeeping of the watermark by smearing block cipher methodology with fixed length blocks of 128 bits. For improved safety a concentrated key length of 256 bits is engendered by employing ECDHP. Energy compaction scrutiny of DCT produces the essential transform coefficients. Using this characteristic a reduced fraction of coefficients is attained with big magnitude. Quantizing auxiliary coefficients root for analogous re-construction. Re-watermarking model uses the sequential inclusion approach by providing insertion flexibility to the owner of image.

5. PROPOSED MODEL, EXPERIMENTAL RESULTS AND DISCUSSION

5.1. Experimental Environment

A total of one hundred test images are taken for embedding watermarks. Color images of .jpeg format form the test images. Four different image dimensions are identified for embedding which includes: 512×512, 640×480, 800×600 and 1024×768. Each dimension includes 25 different images. Owner watermarks embedded are are shown in Table 5. Size of watermark varies from 256–3328. Owner details include Owner Identification Number (OID), Owner Name (ON), Owner House Number (OHN), Owner Sector (OSE), Owner City (OC), Owner State (OST), Owner Mobile Number (OMN), Owner E-mail (OEM) and Owner Country (OCY). Multiple owner details are generated by assigning the owner details sequentially. Encrypted owner details are generated in multiple of 128 bits as per the block size specification of AES.

Watermark embedding is achieved by combining different owner details. In re-watermarking multiple watermarks are implanted in a sequential manner. Re-watermarking model uses the successive insertion method to deliver flexibility by defining the number of watermarks to be inserted in the image.

5.2. Proposed Model

For embedding and extracting watermark content (E_c) from cover Image (I), various operations performed are depicted in Figure 6 and Figure 7. Mid Frequency Coefficients (M_{FC}) are quantized using DCT in Block Size (B_s) of 4×4. Partial IDCT and second DCT are applied for block determination (B_D). The RGB color space is converted to YUV color space for each 4×4 block using equations (20).

$$\begin{aligned} Y &= 0.299 \times R + 0.587 \times G + 0.114 \times B \\ U &= 0.596 \times R - 0.275 \times G - 0.321 \times B \\ V &= 0.212 \times R - 0.523 \times G - 0.311 \times B \end{aligned} \quad (20)$$

5.3. Experimental Results

Quantitative parameters are analyzed for identifying the effectiveness of the proposed approach. The parameters include Peak Signal to Noise Ratio (PSNR), Structure Similarity Index (SSIM), Correlation Coefficient (CC), Entropy (E), Embedding Processing Time (EPT) and Retrieval Processing Time (RPT). The statistical analysis data SAD containing minimum (MN), maximum (MX) and mean (ME) values are evaluated for each parameter.

Quantitative parameters are mathematically defined image quality measures which play a vital role depending upon the image processing applications they are applied in. The quality measures are independent of the perceptual conditions and specific observers. PSNR is

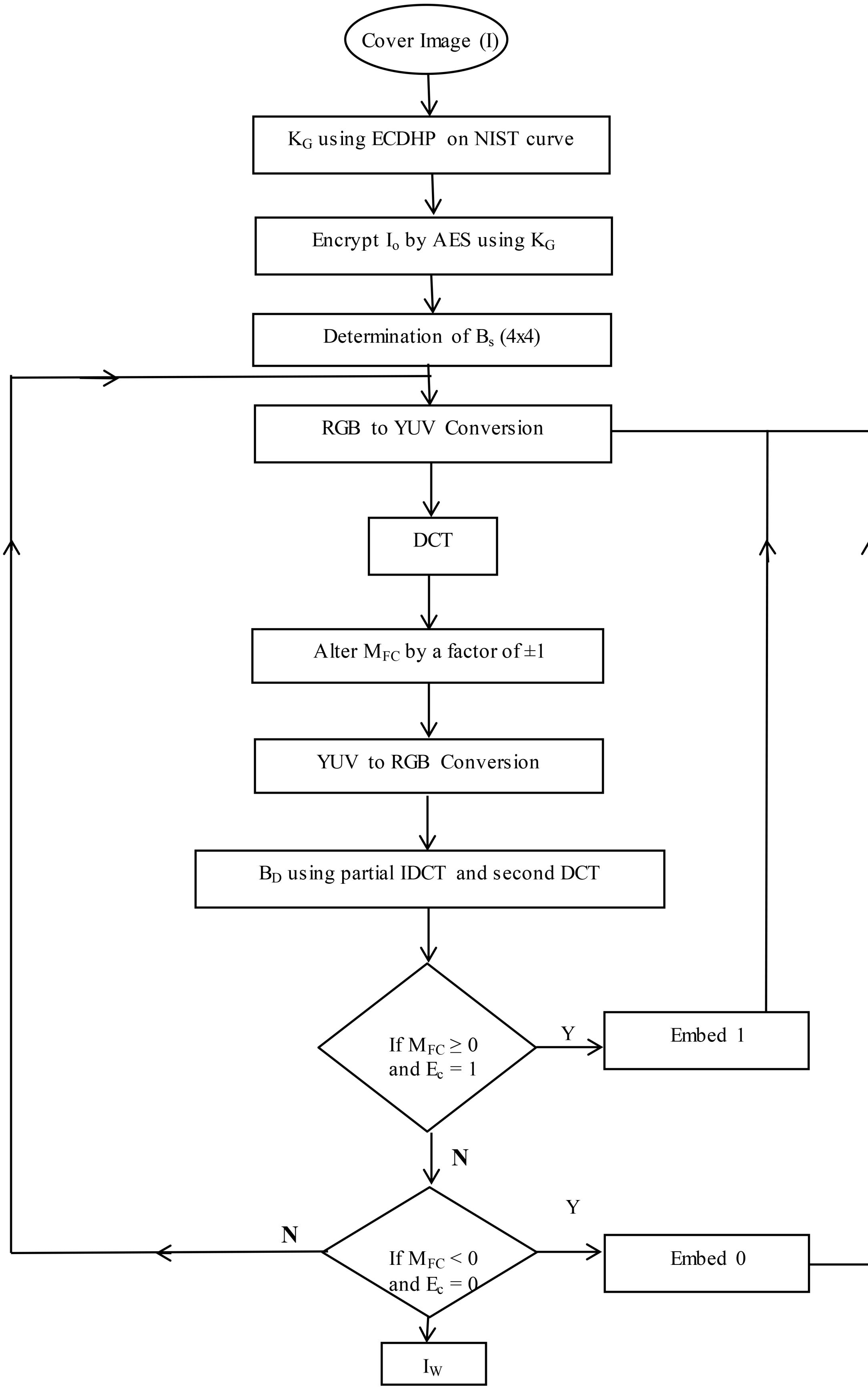

Fig. 6. Watermark Embedding Algorithm

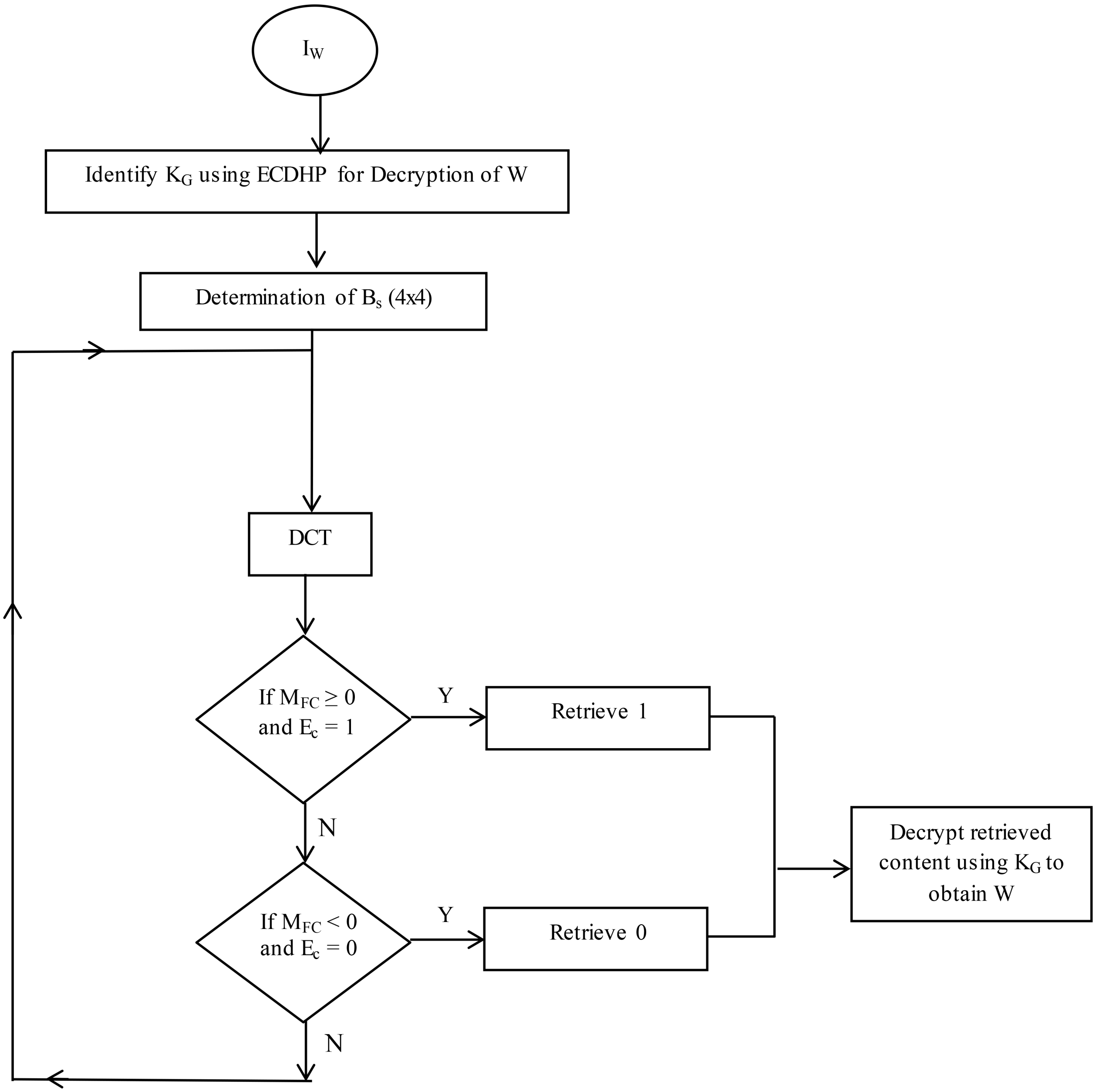

Fig. 7. Watermark Retrieval Algorithm

created on pixel difference based measure. In this original and watermarked images are compared in terms of undistorted reference signal and error signal. SSIM on the other hand is based on Human Visual System measure. This measure is closely related to the perception of human eye in terms of luminance, contrast and comparative structure of two images. In CC correlation of pixels is used as a measure of the image quality measure. Entropy is used to predict the image coding quality for different embedding rates. It measures the disorganized occurrence of watermarked pixels in each row and column and to increase the image visibility.

1) PSNR PSNR is a commonly used measure for determining the quality of images. PSNR computes the peak signal to noise ratio between two images. The ratio factor is used for quality determination among cover image and watermarked image. PSNR for image is calculated in decibels (dB) using the equation [61] (21).

$$\mathrm{PSNR} = 10\log_{10}\frac{(2^N - 1)^2}{\mathrm{MSE}} \tag{21}$$

N is the maximum bit size for a pixel, MSE is Mean Square Error.

PSNR is calculated for all image dimensions with varying watermark size. High values of PSNR obtained imply that the generated image contains less noise. Inverse relation exists between MSE and PSNR such that a lower value of MSE results in high PSNR whereas a higher value of MSE results in low PSNR.

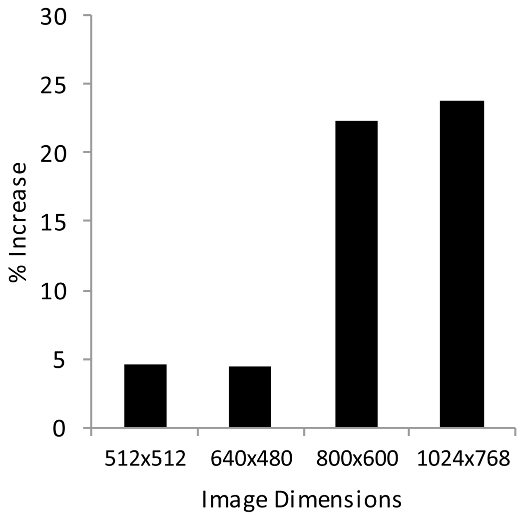

Fig. 8. % Increase in PSNR for different image dimensions.

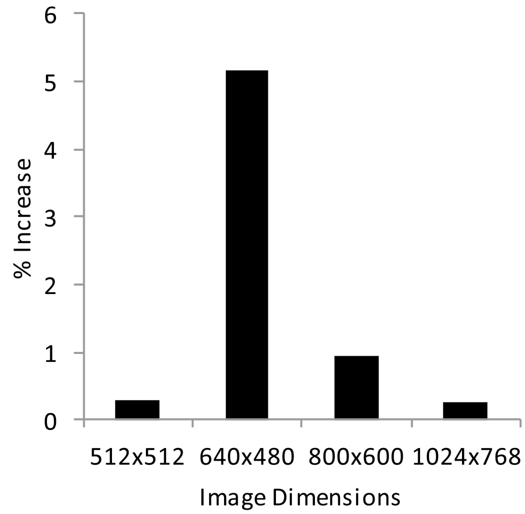

Fig. 9. % Increase in SSIM for different image dimensions.

TABLE 6.
Comparative analysis of PSNR obtained with previous approaches.

Image Dimensions	Proposed Approach	Previous Approach	% Increase
512×512	50.69	48.5 [62]	4.52
640×480	51.28	49.09 [63]	4.46
800×600	53.17	43.48 [64]	22.29
1024×768	55.22	44.6 [65]	23.81

TABLE 7.
Comparative analysis of SSIM obtained with previous approaches.

Image Dimensions	Proposed Approach	Previous Approach	% Increase
512×512	0.99894	.99600 [67]	.30
640×480	0.99908	.99250 [68]	5.17
800×600	0.99932	.99000 [69]	.94
1024×768	0.99957	.99710 [70]	.25

Average PSNR results obtained are: 50.69 for 512×512 images, 51.28 for 640×480 images, 53.17 for 800×600 images and 55.22 for 1024×768. The results ascertain creation of good quality watermarked images. It is also observed that with increasing image dimensions PSNR is also getting increased. Comparative analysis of PSNR obtained using our proposed approach with other approaches identified from literature is shown in Table 6.

M_X PSNR % increase of 23.81 is observed for 1024×768 images while MN PSNR % increase of 4.46 is observed for 640×480 images. The results obtained using the proposed approach delivers a PSNR higher than the existing techniques, thereby displaying a significant improvement. % increase in PSNR for different image dimensions is shown in Figure 8.

2) SSIM SSIM calculates the similarity among two images. It is based on the notion of HVS that measure the variation of structure between the original and the watermarked image. It matches luminance, contrast and structure among two images. Maximum value of 1 is attained if the two images are completely alike. SSIM is defined by the equation [9] (22).

$$\mathrm{SSIM}(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \tag{22}$$

where, x, y are the image pixel positions; μ_x, μ_y are the mean values w.r.t. x and y; σ_x, σ_y are the standard deviation values w.r.t. x and y; C_1 and C_2 are the stability constants. SSIM is calculated for all image dimensions varying watermark size. Comparative analysis of SSIM obtained using proposed approach with previous approaches identified from literature is shown in Table 7.

Structural data present in an image have strong inter-pixel dependencies among spatial content. It lies in the range of -1 and 1. These dependencies carry significant evidence about the structure of the objects in the image. M_X SSIM % increase of 5.17 is observed for 640×480 images while M_N SSIM % increase of .25 is observed for 1024×768 images. Experimental results state an improvement of SSIM index in comparison to the previous approaches. If two images are alike by SSIM then perceptual quality of watermarked image is considered to be of good quality. % Increase in SSIM for different image dimensions is shown in Figure 9.

3) CC CC parameter identifies the association among two images. A positive correlation creates a CC value close to $+1$ while a negative correlation creates a CC value close to -1. The CC between original image and watermarked image computes image deformation at

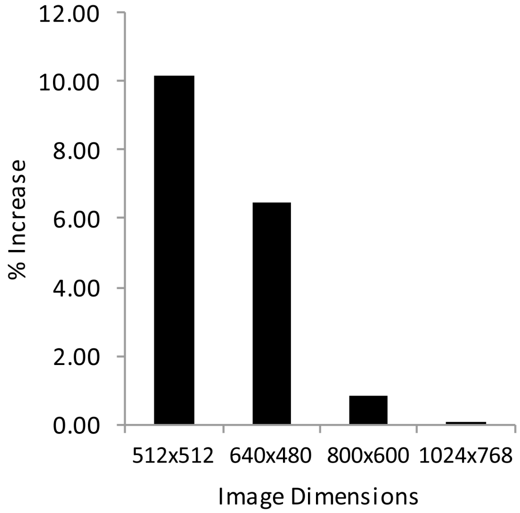

Fig. 10. % Increase in CC for different image dimensions.

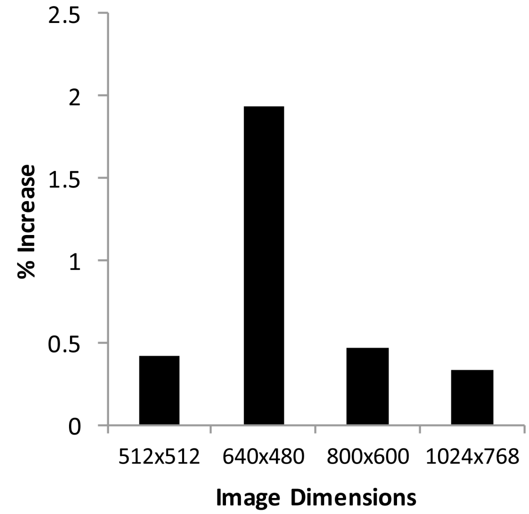

Fig. 11. % Increase in NPCR for different image dimensions.

TABLE 8.
Comparative analysis of CC obtained with previous approaches.

Image Dimensions	Proposed Approach	Previous Approach	% Increase
512×512	.99969	0.9074 [72]	10.17
640×480	.99978	0.9389 [71]	6.48
800×600	.99985	0.99166 [73]	0.83
1024×768	.99985	0.9992 [74]	0.07

TABLE 9.
% Increase in NPCR for different image dimensions.

Image Dimensions	% Increase
512×512	0.42
640×480	1.94
800×600	0.47
1024×768	0.33

pixels level. CC is calculated by the equation [71] (23).

$$C_{ab} = \frac{\frac{1}{r*c}\sum\sum(A_{i,j}-\bar{A})(B_{i,j}-\bar{B})}{\sqrt{\frac{1}{r*c}\sum\sum(A_{i,j}-\bar{A})^2}\sqrt{\frac{1}{r*c}\sum\sum(B_{i,j}-\bar{B})^2}} \quad (23)$$

$A_{i,j}$ and $B_{i,j}$ are the pixels in the ith row and jth column of images A and B; $\bar{A}$ is the mean of A while $\bar{B}$ is mean of B; r and c are the width and height of an image. CC is measured for all image dimensions with varying watermark size. Comparative analysis of CC obtained with previous approaches is shown in Table 8.

The closer CC value is to one, the better it is. Our approach generates a high positive CC which reveals a strong association among host image and watermarked image. M_X CC % increase of 10.17 is observed for 512×512 images while M_N CC % increase of .07 is observed for 1024×768 images. Experimental results state an improvement of CC in comparison to the previous approaches. % Increase in CC for different image dimensions is shown in Figure 10.

4) NPCR NPCR determines the total number of pixels altered between original image (I) and watermarked image (I'). It calculates the percentage of dissimilar pixel quantities between images. NPCR is calculated by equation [75] (24)

$$\text{NPCR} = \frac{\sum_{i=1}^{m}\sum_{i=1}^{n} p_{i,j}}{m*n} * 100\% \quad (24)$$

where,

$$p_{i,j} = 0, \text{ if } I_{i,j} = I'_{i,j}$$
$$1, \text{ if } I_{i,j} \neq I'_{i,j}$$

m, n are the width and height of the image; $p_{i,j}$ is an array of same size as I and I'. NPCR is evaluated for all image dimensions with varying watermark size. Average NPCR results obtained are: .11282 for 512×512 images, 0.10254 for 640×480 images, 0.07732 for 800×600 images and 0.05803 for 1024×768. Comparative ratio proportion reveals % increase in NPCR obtained using proposed approach with previous image encryption approaches [76–79]. % Increase in NPCR for different image dimensions is shown in Table 9.

NPCR parameter is used commonly in image encryption. The parameter identifies the number of pixels change rate between two ciphered images. For good NPCR encrypted image the change rate should be close to 100. For the first time NPCR parameter is explored in the field of watermarking. Since watermarking aims at prevention of image distortion between original and the watermarked image, so a good NPCR watermarked image will give value close to 0. Our average NPCR outcome for different image dimensions reveals a good assessment. M_X NPCR % increase of 1.94 is observed for 640×480 images while M_N NPCR % increase of .09 is observed for 1024×768 images. % Increase in NPCR for different image dimensions is shown in Figure 11.

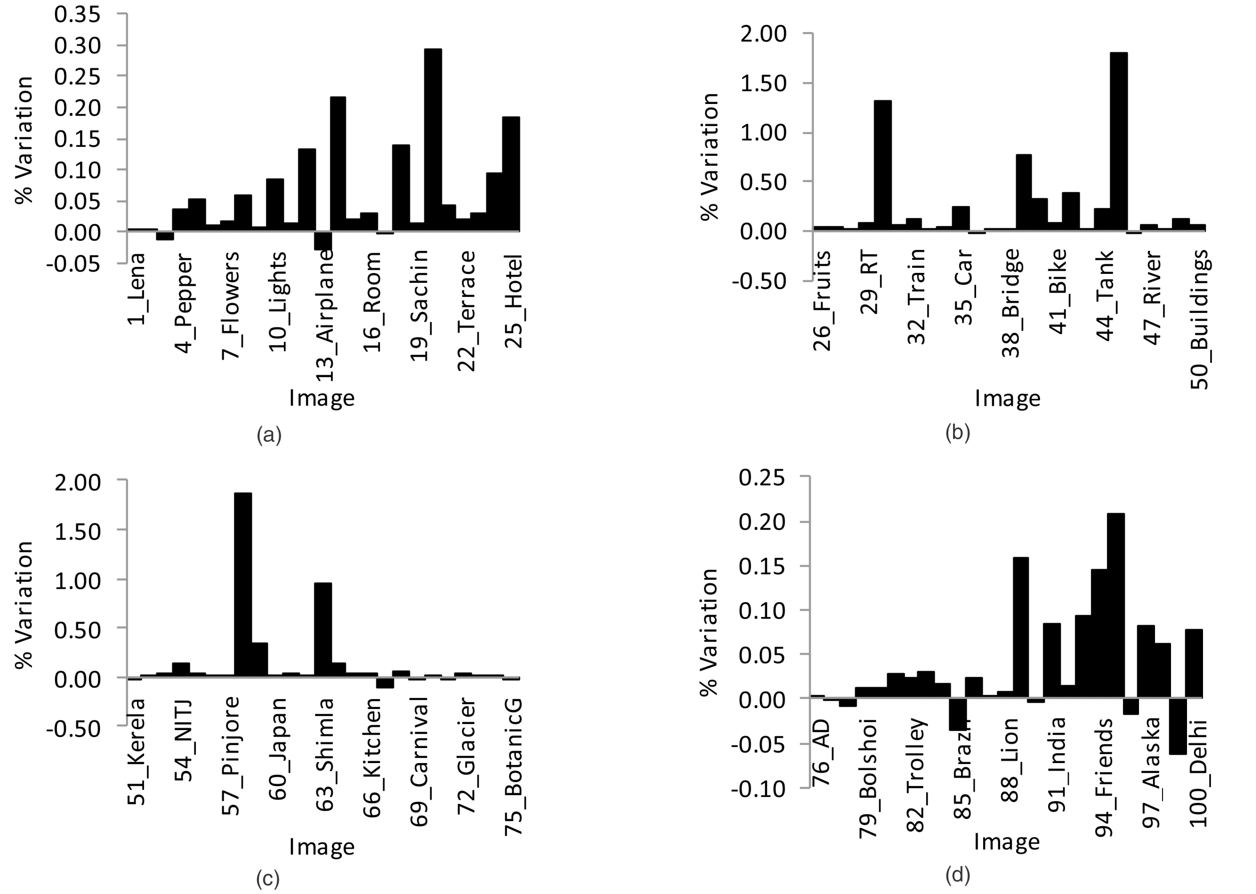

Fig. 12. % Variation in Entropy between original images and complete watermarked images for dimensions. (a) 512×512; (b) 640×480; (c) 800×600; (d) 1024×768.

5) Entropy Entropy is a statistical measure of uncertainty defined by the equation [80] (25)

$$E_G = \sum_{x \in G}^{n} p(x) \log\left(\frac{1}{p(x)}\right) \tag{25}$$

G is the data raised from a particular domain and $p(x)$ is the probability of sample in the group G. Entropy parameter ascertains existence of watermarks' imperceptibility. A watermarked image having high entropy has less perceivable distortion to human eye than an image with low entropy.

Entropy is estimated for all image dimensions with varying watermark size. Average Entropy results obtained are: 7.3847 for 512×512 images, 7.3653 for 640×480 images, 7.4225 for 800×600 images and 7.4733 for 1024×768 images. % Variation in Entropy between original images and complete watermarked images for all image dimensions are shown in Figure 12. Results show that the watermarks embedded in the image are highly imperceptible as the entropy values obtained are slightly more than the original image entropy. A higher disorder implies that more information can be embedded in the image without being perceived.

6) EPT and RPT EPT is the total computational time taken by the proposed watermarking scheme. It is measured in milliseconds (ms). The processing time achieved using the proposed approach depicts a small embedding time complexity as shown in Figure 13.

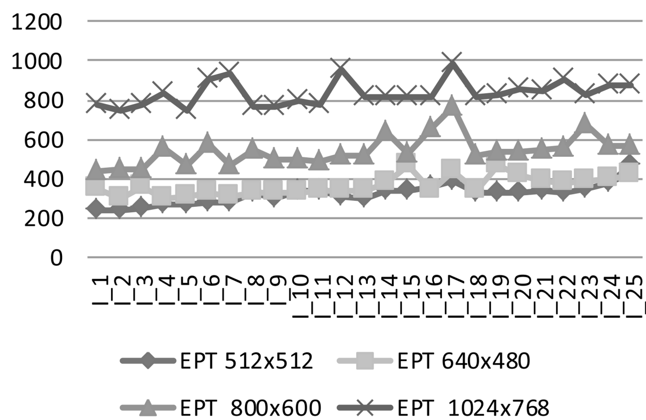

Fig. 13. % EPT for various image dimensions.

RPT is the total computational time taken by the proposed watermarking scheme. It is measured in milliseconds (ms). The processing time achieved using the proposed approach depicts a small retrieving time complexity as shown in Figure 14.

7) Robustness In order to test the robustness of the proposed approach, various attacks are launched against

TABLE 10.
NC for various attacks.

Attack	Previous Approach 512 × 512	512 × 512	640 × 480	800 × 600	1024 × 768
Salt and Pepper Noise	.9805	.9857	.9887	.9896	.9912
Gaussian Noise	.9800	.9859	.9873	.9894	.9921
Cropping	.9177	.9265	.9289	.9345	.9412
JPEG Compression	.9898	.9917	.9939	.9947	.9986
Median Filtering	.9112	.9225	.9312	.9319	.9418

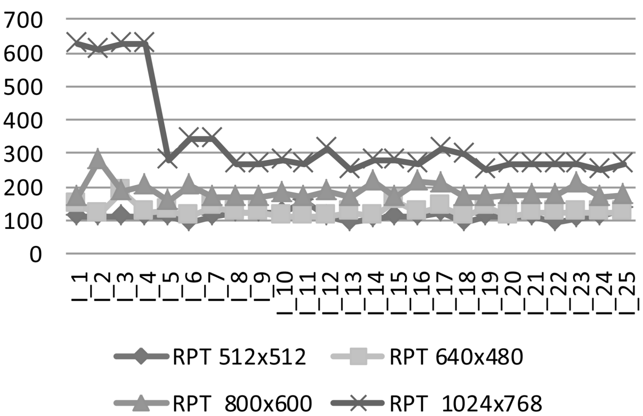

Fig. 14. % RPT for various image dimensions.

the watermarked image. These attacks include Salt and Pepper Noise, Gaussian Noise, Cropping, JPEG Compression and Median Filtering. Normalized Correlation (NC) performance of proposed algorithm against attacks on watermark embedded for a set of all image dimensions is shown in Table 10.

6. CONCLUSIONS

This paper proposes the problem of semi-blind and secure digital watermarking for authentic cation of images. It generates solution by providing confidentiality, integrity, and authenticity to the watermarked image. The objective is achieved by integrating digital watermarking & cryptography together in order to insert the secret information to gain a high level of privacy & efficiency. AES encrypted watermark with a secret key bundle makes it very challenging for the attacker to identify and hinder the watermark saved inside host image. ECDHP generates secret key based on discrete logarithm for solving key distribution problem among multiple owners and distributers. Insertion and removal of secure watermark using DCT domain provides low computational complexity and fast speed. The performances of the secure watermarking technique are compared on the basis of PSNR, SSIM, CC, NPCR and Entropy values. Quantitative analysis of image quality parameters reveals effectiveness of the proposed approach.

REFERENCES

[1] M. H. Pi, C. H. Li, and H. Li
A novel fractal image watermarking
IEEE Transactions on Multimedia, Vol. 8, No. 3, 2006, pp. 488–499.

[2] Y. Hu and B. Jeon
Reversible Visible Watermarking and Lossless Recovery of Original Images
IEEE Transactions on Circuits and Systems for Video Technology, Vol. 16, No. 11, 2006, pp. 1423–1429.

[3] D. M. Thodi and J. J. Rodriguez
Expansion Embedding Techniques for Reversible Watermarking
IEEE Transactions on Image Processing, Vol. 16, No. 3, 2007, pp. 721–730.

[4] P. Y. Lin, J. S. Lee, and C.C. Chang
Dual Digital Watermarking for Internet Media Based on Hybrid Strategies
IEEE Transactions on Circuits and Systems for Video Technology, Vol. 19, No. 8, 2009, pp. 1169–1177.

[5] T. Y. Liu and W. H. Tsai
Generic Lossless Visible Watermarking—A New Approach
IEEE Transactions on Image Processing, Vol. 19, No. 5, 2010, pp. 1224–1235.

[6] L. Kocarev, Z. Galias, and S. Lian
Intelligent Computing Based on Chaos
Springer, 2009.

[7] A. K. Parthasarathy and S. Kak
An Improved Method of Content Based Image Watermarking
IEEE Transactions on Broadcasting, Vol. 53, No. 2, 2007, pp. 468–479,

[8] L. O. M. Kobayashi, S. S. Furuie, and P. S. L. M. Barreto
Providing Integrity and Authenticity in DICOM Images: A Novel Approach
IEEE Transactions on Information Technology in Biomedicine, Vol. 13, No. 4, 2009, pp. 582–589.

[9] C. Chin-Chen and H. Chou
A New Public-Key Oblivious Fragile Watermarking for Image Authentication Using Discrete Cosine Transform
In Second International Conference on Future Generation Communication and Networking Symposia, 2008, pp. 11–14.

[10] C. Fei, R. H. Kwong, D. Kundur, and F. Chuhong
A Hypothesis Testing Approach to Semifragile Watermark-Based Authentication
IEEE Transactions on Information Forensics and Security, Vol. 4, No. 2, 2009, pp. 179–192.

[11] K. C. Liu and C. H. Chou
Robust and transparent watermarking scheme for colour images
IET Image Processing, Vol. 3, No. 4, 2009, pp. 228–242.

[12] T. Jen-Sheng, H. Win-Bin, and K. Yau-Hwang
On the Selection of Optimal Feature Region Set for Robust Digital Image Watermarking
IEEE Transactions on Image Processing, Vol. 20, No. 3, 2011, pp. 735–743.

[13] P. S. Huang, C. S. Chiang, C. P. Chang, and T. M. Tu
Robust spatial watermarking technique for colour images via direct saturation adjustment
IEE Proceedings—Vision, Image and Signal Processing, Vol. 152, No. 5, 2005, pp. 561–574.

[14] S. K. Singh, S. Kumar, M. Srivastava, A. Chandra, and S. Srivastava
Wavelet Based Robust Digital Watermarking Technique Using Reverse Additive Algorithm (RAA)
In Third UKSim European Symposium on Computer Modeling and Simulation, 2009, pp. 241–244.

[15] S. P. Mohanty, E. Kougianos, and N. Ranganathan
VLSI architecture and chip for combined invisible robust and fragile watermarking
IET Computers & Digital Techniques, Vol. 1, No. 5, 2007, pp. 600–611.

[16] G. Karakonstantis, N. Banerjee, and K. Roy
Process-Variation Resilient and Voltage-Scalable DCT Architecture for Robust Low-Power Computing
IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 18, No. 10, 2010, pp. 1461–1470.

[17] W. C. Chu
DCT-based image watermarking using subsampling
IEEE Transactions on Multimedia, Vol. 5, No. 1, 2003, pp. 34–38.

[18] X. Jun and W. Ying
Multiple Watermarking Based on Spread Transform
In 8th International Conference on Signal Processing, 2006, pp. 1–4.

[19] Z. Dong, W. Sha, and Z. Jiying
RST Invariant Image Watermarking Algorithm with Mathematical Modeling and Analysis of the Watermarking Processes
IEEE Transactions on Image Processing, Vol. 18, No. 5, 2009, pp. 1055–1068.

[20] Z. Ying, X. Jun, and W. Ying
Side informed image watermarking algorithm with high security
In IEEE Youth Conference on Information, Computing and Telecommunication, 2009, pp. 395–398.

[21] Y. Tan, L. Tang, Z. Gao, P. Sun, X. Yang, and Y. Li
A Rotation Resistant Image Watermarking Algorithm via Circle
In Eighth International Conference on Computational Intelligence and Security (CIS), 2012, pp. 461–463.

[22] P. Viswanathan, and P. V. Krishna
A Joint FED Watermarking System using Spatial Fusion for Verifying the Security Issues of Teleradiology
IEEE Journal of Biomedical and Health Informatics, Vol. 18, No. 3, pp. 753–764, 2014.

[23] V. M. Potdar, H. Song, and E. Chang
A survey of digital image watermarking techniques
In 3rd IEEE International Conference on Industrial Informatics, 2005, pp. 709–716.

[24] T. Stutz, F. Autrusseau, and A. Uhl
Non-Blind Structure-Preserving Substitution Watermarking of H.264/CAVLC Inter-Frames
IEEE Transactions on Multimedia, Vol. 16, No.5, pp. 1337–1349, 2014.

[25] L. Zhang, F. Qian, Y. Gao, and Y. Zhu
A New Integration Scheme of Robust and Fragile for Secured Digital Watermarking
International Colloquium on Computing, Communication, Control, and Management, 2008, pp. 312–316.

[26] Y.-W. Ding, Z. Lin, and L. Wang
A Multipurpose Public-Key Cryptosystem Based Image Watermarking,
In 4th International Conference on Wireless Communications, Networking and Mobile Computing, 2008, pp. 1–4.

[27] RBI
FAQ on Cheque Truncation Project in the National Capital Region
Department of Payment and Settlement Systems, 2010.

[28] RBI
Payment and Settlement Systems and Information Technology
Reserve Bank of India Annual Report 12-13, 2013. pp. 128–139

[29] R. Eswaraiah, and E. Sreenivasa Reddy
Robust medical image watermarking technique for accurate detection of tampers inside region of interest and recovering original region of interest
IET Image Processing, Vol. 9, No. 8, 2015, pp. 615–625.

[30] X. Li, X. Sun and L. Quansheng
Image Integrity Authentication Scheme Based on Fixed Point Theory
IEEE Transactions on Image Processing, Vol. 24, No. 2, 2015, pp. 632–635

[31] A. B. Jeng and C. Lo-Yi
How to enhance the security of e-Passport
In International Conference on Machine Learning and Cybernetics, 2009, pp. 2922–2926.

[32] S. Kundra, A. Dureja, and R. Bhatnagar
The study of recent technologies used in E-passport system
In IEEE Global Humanitarian Technology Conference—South Asia Satellite (GHTC-SAS), 2014, pp. 141–146.

[33] M. Q. Saeed, A. Masood, and F. Kausar
Securing ePassport system: A proposed Anti-Cloning and Anti-Skimming Protocol
In 17th International Conference on Software, Telecommunications & Computer Networks, 2009, pp. 90–94.

[34] K. D. Akdemir, D. Karakoyunlu, and B. Sunar
Non-linear error detection for elliptic curve cryptosystems
IET Information Security, Vol. 6, No. 1, 2012, pp. 28–40.

[35] L. Jyu-Yuan and H. Chih-Tsun
Energy-Adaptive Dual-Field Processor for High-Performance Elliptic Curve Cryptographic Applications
IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 19, No. 8, 2011, pp. 1512–1517.

[36] D. M. Schinianakis, A. P. Fournaris, H. E. Michail, A. P. Kakarountas, and T. Stouraitis
An RNS Implementation of an Elliptic Curve Point Multiplier
IEEE Transactions on Circuits and Systems, Vol. 56, No. 6, pp. 2009, 1202–1213.

[37] NIST
Digital Signature Standard
In Federal Information Processing Standards Publications FIPS PUB 186-2, 2000, pp. 1–73.

[38] NIST
Mathematical routines for the NIST prime elliptic curves
In National Security Agency, 2010, pp. 1–43.

[39] NIST
Recommended Elliptic Curves for Federal Government Use http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf, Date of Accession 19-11-2013.

[40] K. Ananyi, H. Alrimeih, and D. Rakhmatov
Flexible Hardware Processor for Elliptic Curve Cryptography Over NIST Prime Fields
IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 17, No. 8, 2009, pp. 1099–1112.

[41] O. S. Althobaiti and H. A. Aboalsamh
An enhanced Elliptic Curve Cryptography for biometric
In 7th International Conference on Computing and Convergence Technology (ICCCT), 2012, pp. 1048–1055.

[42] L. Tawalbeh, M. Mowafi, and W. Aljoby
Use of elliptic curve cryptography for multimedia encryption
IET Information Security, Vol. 7, No. 2, 2013, pp. 67–74.

[43] A. Cilardo, L. Coppolino, N. Mazzocca, and L. Romano
Elliptic Curve Cryptography Engineering
Proceedings of the IEEE, Vol. 94, No. 2, 2006, pp. 395–406.

[44] M. Amara and A. Siad
Elliptic Curve Cryptography and its applications
In 7th International Workshop on Systems, Signal Processing and their Applications (WOSSPA), 2011, pp. 247–250.

[45] A. Sachan, S. Emmanuel, A. Das, and M. S. Kankanhalli
Privacy Preserving Multiparty Multilevel DRM Architecture
In 6th IEEE Consumer Communications and Networking Conference, 2009, pp. 1–5.

[46] D. Mishra and S. Mukhopadhyay
Privacy preserving hierarchical content distribution in multiparty multilevel DRM
In World Congress on Information and Communication Technologies (WICT), 2012, pp. 525–530.

[47] L. Harn, W. J. Hsin, and M. Mehta
Authenticated Diffie-Hellman key agreement protocol using a single cryptographic assumption
IEE Proceedings—Communications, Vol. 152, No. 4, 2005, pp. 404–410.

[48] G. P. Biswas
Diffie-Hellman technique: extended to multiple two-party keys and one multi-party key
IET Information Security, Vol. 2, No. 1, 2008, pp. 12–18.

[49] M. Abid and H. Afifi
Secure E-Passport Protocol Using Elliptic Curve Diffie-Hellman Key Agreement Protocol
In Fourth International Conference on Information Assurance and Security, 2008, pp. 99–102.

[50] J. R. Vacca
Computer and Information Security
1st ed.: Morgan Kaufmann Publishers, 2009.

[51] X. Li, J. Chen, D. Qin, and W. Wan
Research and realization based on hybrid encryption algorithm of improved AES and ECC
In International Conference on Audio Language and Image Processing (ICALIP), 2010, pp. 396–400.

[52] NIST
Advanced Encryption Standard
In Federal Information Processing Standards, 2001, pp. 1–47.

[53] W. E. Burr
Selecting the Advanced Encryption Standard
IEEE Security & Privacy, Vol. 1, No. 2, 2003, pp. 43–52.

[54] M. Mozaffari-Kermani and A. Reyhani-Masoleh
Efficient and High-Performance Parallel Hardware Architectures for the AES-GCM
IEEE Transactions on Computers, Vol. 61, No. 8, 2012, pp. 1165–1178.

[55] R. Banu and T. Vladimirova
Fault-Tolerant Encryption for Space Applications
IEEE Transactions on Aerospace and Electronic Systems, Vol. 45, No. 1, 2009, pp. 266–279.

[56] L. Bin and B. M. Baas
Parallel AES Encryption Engines for Many-Core Processor Arrays
IEEE Transactions on Computers, Vol. 62, No. 3, pp. 2013, 536–547.

[57] R. Setchi, I. Jordanov, R. J. Howlett, and L. C. Jain
Knowledge-Based and Intelligent Information and Engineering Systems
Springer, 2010.

[58] S. P. Noolu and M. S. Baghini
Comments on An Analog 2-D DCT Processor
IEEE Transactions on Circuits and Systems for Video Technology, Vol. 20, No. 8, 2010, pp. 1162–1163.

[59] T. Dutoit and F. Marques
Applied Signal Processing
Springer, 2009.

[60] E. L. Tan, W. S. Gan, and S. K. Mitra
Fast arbitrary resizing of images in the discrete cosine transform domain
IET Image Processing, Vol. 5, No. 1, 2011, pp. 73–86.

[61] E. Walia and A. Suneja
Fragile and blind watermarking technique based on Weber's law for medical image authentication
Computer Vision, Vol. 7, No. 1, 2013, pp. 9–19.

[62] J. Hammerle-Uhl, C. Koidl, and A. Uhl
Multiple blind re-watermarking with quantisation-based embedding
In 18th IEEE International Conference on Image Processing (ICIP), 2011, pp. 265–268.

[63] R. Rosenbaum, G. Fuchs, and H. Schumann
Region-wise meta-data in JPEG2000-encoded imagery
In 5th International Conference on Visual Information Engineering, 2008, pp. 741–746.

[64] E. Halici and A. A. Alatan
Watermarking for depth image based rendering
In IEEE International Conference on Image Processing (ICIP), 2009, pp. 4217–4220.

[65] T. Hui Li, L. Zhengguo, T. Yih Han, S. Rahardja, and Y. Chuohuo
A Perceptually Relevant MSE-Based Image Quality Metric
IEEE Transactions on Image Processing, Vol. 22, No. 11, 2013, pp. 4447–4459.

[66] T. Hui Li, L. Zhengguo, T. Yih Han, S. Rahardja, and Y. Chuohuo
A Perceptually Relevant MSE-Based Image Quality Metric
IEEE Transactions on Image Processing, Vol. 22, No. 11, 2013, pp. 4447–4459.

[67] A. Kunhu and H. Al-Ahmad
Multi watermarking algorithm based on DCT and hash functions for color satellite images
In 9th International Conference on Innovations in Information Technology (IIT), 2013, pp. 30–35.

[68] H. Heechul and S. Kwanghoon
Automatic illumination and color compensation using mean shift and sigma filter
IEEE Transactions on Consumer Electronics, Vol. 55, No. 3, pp. 2009, 978–986.

[69] R. F. Lopes, C. D. M. Regis, W. T. A. Lopes, and M. S. de Alencar
AdaptVoD—An Adaptive Video-on-Demand Platform for Mobile Devices
In 5th FTRA International Conference on Multimedia and Ubiquitous Engineering (MUE), 2011, pp. 257–262.

[70] D. V. S. X. De Silva, W. A. C. Fernando, S. T. Worrall, and A. M. Kondoz
A novel depth map quality metric and its usage in depth map coding
In 3DTV Conference: The True Vision—Capture, Transmission and Display of 3D Video (3DTV-CON), 2011, pp. 1–4.

[71] S. Philipp, K. Stephan, E. Wolfgang, and T. Niels
Semi-automatic registration of videos for improved watermark detection
In Proceedings of the first annual ACM SIGMM conference on Multimedia systems Phoenix, Arizona, USA: ACM, 2010, pp. 23–34.

[72] H. A. Al-Otum and A. O. Al-Taba'a
Color image copyright ownership protection based on a multi-spectral selective pixel-wise watermarking technique
In 3rd International Symposium on Communications, Control and Signal Processing (ISCCSP), 2008, pp. 544–549.

[73] L. Cheng-Liang and C. Yi-Shiang
The application of intelligent system to digital image forensics
In International Conference on Machine Learning and Cybernetics, 2009, pp. 2991–2998.

[74] S. Kwong, H. Yuan, J. Liu, and J. Sun
A Novel Distortion Model and Lagrangian Multiplier for Depth Maps Coding
IEEE Transactions on Circuits and Systems for Video Technology, Vol. 25, No. 99, 2014, pp. 443–451.

[75] A. Umamageswari and G. R. Suresh
Security in medical image communication with arnold's cat map method and reversible watermarking
In International Conference on Circuits, Power and Computing Technologies (ICCPCT), 2013, pp. 1116–1121.

[76] M. S. El-Mahallawy, E. A. Hagras, A. Z. Eldin, and M. W. Fakhr
Robust Blind and Secure Biometric Watermarking Based on Partial Multi-Map Chaotic Encryption
In 4th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2011, pp. 1–5.

[77] K. P. Narendra, P. Vinod, and K. S. Krishan
Diffusion-substitution based gray image encryption scheme
Digital Signal Processing, Vol. 23, No. 3, 2013, pp. 894–901.

[78] N. K. Pareek, V. Patidar, and K. K. Sud
Substitution-diffusion based Image Cipher
International Journal of Network Security & Its Applications, Vol. 3, No. 2, 2011, pp. 149–160.

[79] S. M. Seyedzadeh and Y. Hashemi
Image encryption algorithm based on Choquet Fuzzy Integral with self-adaptive pseudo-random number generator
In 11th International Conference on Intelligent Systems Design and Applications (ISDA), 2011, pp. 642–647.

[80] Y. Qiu, Z. Yana, Y. Cheng, and L. Wei
Information Entropy Used in Digital Watermarking
In Symposium on Photonics and Optoelectronics (SOPO), 2012, pp. 1–4.

Vineet Mehan received the B.Tech. degree in Information Technology from Kurukshetra University in 2003. He received the M.E. degree in Computer Science and Engineering from NITTTR, Panjab University in 2008. He completed Ph.D. degree in Computer Science and Engineering from Dr. B.R. Ambedkar National Institute of Technology, Jalandhar in 2016. His research interests include Image Processing, Watermarking and Cryptographic Algorithms.