International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 4, Issue 4, July - August 2015 **ISSN 2278-6856**

Self Generative Passcode for Triple-Stegging using Discrete Wavelet Transform (DWT) and Elliptic Curve Cryptography (ECC)

Shivanand S. Gornale[1], Nuthan A.C[2]

[1]Department of Computer Science, School of Mathematic and Computing Sciences, Rani Chennamma University, Belagavi, Karnataka, India.

[2]Department of ECE, GMIT, Bharathinagara, Karnataka, India.
Research Scholar, Jain University, Bangalore.

Abstract
Preserving sensitive information is an integral part of present communication world. This paper deals with one such improved method for embedding sensitive data in color images. To provide enhanced security of data the proposed technique hybrids the cryptography and Steganography where encrypted data (using cryptography) is embedded into n image(cover media) using Triple- Stegging and DWT. This technique handles the image quality and robustness and fault tolerance of implementation efficiently.
Keywords: DWT, ECC, Random Number Generator (RNG), Triple-steggimg, LFSR.

1. INTRODUCTION

Information security is defined as the prevention of data from unauthorized access or destruction to provide confidentiality, integrity, and availability [1]. Cryptography and steganography are the two popular methods available to provide security [9-11]. The data which is considered as sensitive are transformed to unrecognizable form using cryptography and steganography while being stored and transmitted. These techniques also take cares message integrity, sender or receiver authentication and secure computation.
In cryptography the sensitive data(text, image, audio, video and so forth) called plaintext is converted to scrambled ciphertext using encryption algorithm and a key [2-4]. The reverse of data encryption is data decryption. Secret key cryptography (Same key for both encryption and decryption) and Public Key cryptography (one key for encryption and another for decryption) are the two different types of cryptography. Hence in Public Key cryptography sender is avoided to share secret key with the receiver as like in Secret Key cryptography. Considering this property of unrevealing secret key the paper narrows to a Public Key Cryptography. ECC is one such example for Public Key Cryptography dealt in Section 3.
Steganography is different from Cryptography. The scrambled nature of a cipher text in cryptography confirms message passing to the hacker i.e. the existence of a secret data is detectable by malicious attackers. The goal of steganography is to embed secret data into a cover image thereby message passing is unknown. Figure 1 shows the typical steganography system. The secret data is embedded in cover image suing stego system encoder and secret key resulting a stego image which is then transmitted or stored. Hence the essence of steganography is it conceals the fact that a secret data is being transmitted without altering the structure of secret message. This stego image is then used by stego decoder to have an estimate of the secret data during reception of retrieval of the data. DWT, DCT and other approaches are used as stego system encoder. This paper uses DWT approach for embedding the secret data which is dealt in Section IV and Section V.

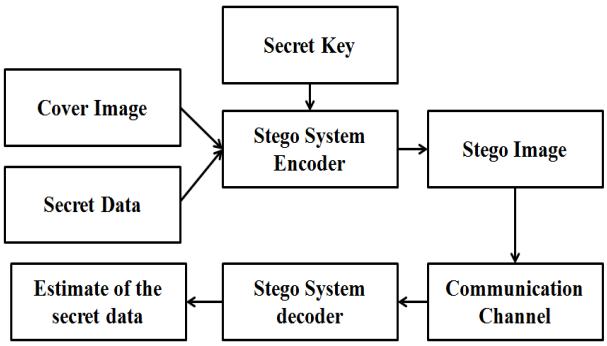

Figure 1 Typical steganography system

2. PROBLEM FORMULATION

The non-recognizable form of cipher text confirms an hacker with the existence of secret data in the hacked message. Therefore in order to hide the existence of such ciphered secret data steganographic method is used to strengthen security level and also to suppress the energy compaction of secret data. This architecture concerns visual quality of the stego-image to be good along with robustness and fault tolerance.
With an objective of securing the data Elliptic curve cryptography is used to convert data into a cipher which is then hidden into an image file. The embedding is applied by modifying the detail coefficients in transform domain of Two-Dimensional Discrete Wavelet Transform (DWT).

2-d DWT enables large capacity of data maintaining good visual quality of the cover image. This is followed by Triple Stegging technique which enhances the security level of the data. A similar work has been carried out using RSA algorithm and double-stegging [7]. As an improvement for the previous work this paper extends number of stages of Steganography from 2 to 3 thus increasing the secrecy of the embedding data. ECC gives a higher security level than RSA with smaller key size [8]. The cover image could be gray scale image [7] or colour image [21]. Since the embedding capacity of colour image is thrice greater than the gray scale image the paper retains colour image as cover image as in [21].

DWT presented uses abstract mathematical setting using special function in [5][7]. Matrix multiplication produces smoother and satisfactory compressed images [6]. Since the nature of image is also matrix, DWT is implemented using matrix multiplication approach in [21]. The same is retained in this work.

Selection of detailed coefficient regions (LH,HL,HH) in DWT is static in [7] i.e., the two regions say HH and HL are selected for embedding the data, then the same regions is maintained throughout the architecture. There was no flexibility to choose the regions. In [21] there was an option to choose the 3 regions based on the 3-bit passcode i.e., given 3 bit passcode 001 the architecture chooses the LH → HL → HH regions for embedding. But the passcode should be given exclusively. As an improvisation, in this paper the 3-bit passcode is generated by the passcode generation block in the architecture and hence there is no necessity to provide passcode externally thereby user himself will not know the passcode to choose the 3 regions.

In [21], only one filter could be used in the architecture. In this paper the architecture is pliable to choose one among 126 wavelet filters. The choice of the wavelet filter is also based on the 7-bits in the passcode generated by passcode generation block.

In [21] the architecture could handle only one-level decomposition in DWT. This paper can undertake one or two level decomposition based on passcode.

Classically, the DWT is defined for sequences with length of some power of 2, and different ways of extending samples of other sizes are needed. Methods for extending the signal include zero-padding, smooth padding, periodic extension, and boundary value replication (symmetrization).The basic algorithm for the DWT is not limited to dyadic length and is based on a simple scheme: convolution and downsampling. As usual, when a convolution is performed on finite-length signals, border distortions arise. Paper [21] does not handle border distortion. This paper handles border distortion efficiently with the mode flexibility based on the passcode.

These enhancements to the previous work [5] [7] [21] recommends integration of Passcode generation block in the architecture. Hence LFSR based Passcode generation block generates 16-bit passcode which is used to handle flexibility in choosing type of wave filters, level of decomposition, order of detailed regions for embedding using triple stegging.

3. ELLIPTIC CURVE CRYPTOGRAPHY [12-17]

Elliptic curve cryptography an approach to public key cryptography was independently suggested by Neil Koblitz and Victor. S. Miller in the year 1985.It is based on the algebraic structure of elliptic curves defined over finite fields. The prime advantage of elliptic curve cryptography is that the key length can be much smaller. Suggested key sizes are in the order of 160 bits providing security equivalent to that of RSA algorithm which uses 1024 bits.

An elliptic curve is a plane curve which is isomorphic to a curve defined by a cubic equation of the form:

$y^2 = x^3 + ax + b$

If $y^2 = x^3 + ax + b$ contains no reprised factors or if $4a^3+27b^2 \neq 0$, then the elliptic curve can be used to form an Abelian group, with the point at infinity as the identity element.

Preliminary operations

1. Point Addition

Consider two distinct points J and K such that $J = (x_J, y_J)$ and $K = (x_K, y_K)$

Let $L = J + K$ where $L = (x_L, y_L)$, then

$x_L = s^2 - x_J - x_K \bmod p$

$y_L = -y_J + s(x_J - x_L) \bmod p$

$s = (y_J - y_K)/(x_J - x_K) \bmod p$,

where s is the slope of the line through J and K.

If K = -J i.e. $K = (x_J, -y_J \bmod p)$ then J + K = O. where O is the point at infinity.

If K = J then J + K = 2J then point doubling equations are used. Also J + K = K + J

2. Point Subtraction

Consider two distinct points J and K such that $J = (x_J, y_J)$ and $K = (x_K, y_K)$, Then

J - K = J + (-K) where $-K = (x_k, -y_k \bmod p)$

3. Point Doubling

Consider a point J such that $J = (x_J, y_J)$, where $y_J \neq 0$

Let L = 2J where $L = (x_L, y_L)$, Then

$x_L = s^2 - 2x_J \bmod p$

$y_L = -y_J + s(x_J - x_L) \bmod p$

$s = (3x_J^2 + a) / (2y_J) \bmod p$,

wheres is the tangent at point J and a is one of the parameters chosen with the elliptic curve

If $y_J = 0$ then 2J = O, where O is the point at infinity.

4. Point multiplication(Using point addition and Point doubling):

Let P be a point on an elliptic curve. Let k be a scalar that is multiplied with the point P toobtain another point Q on the curve. i.e. to find Q = kP.

Steps to perform the ECC encryption and decryption:

1. Select an EC with the domain parameters The domain parameters for Elliptic curve over Fp are p, a, b, G and n. Where 'p' is the prime number defined for finite field 'F_p', 'a' and 'b' are the parameters defining the curve $y^2 \bmod p = x^3 + ax + b \bmod p$, 'G' is the generator point (xG, yG), a point on the elliptic

curve chosen for cryptographic operations, 'n' is the order of the elliptic curve. The scalar for point multiplication is chosen as a number between 0 and n – 1.

2. Choose a generator point G ∈ Ep such that the smallest value of n for which nG=O is a very prime number.
3. Suppose message from 'A' to 'B' is to encrypted. Generate private and public key. Table 1 summarizes the generation of public key using secret key.
4. 'A' encodes the message to point 'Pm' using one-to one mapping .
5. 'A' selects random number 'k' and chooses 'P_B' to encrypt 'Pm'.

$P_C=[(kG),(Pm+kP_B)]$

6. So this gives a pair of points. But since (kG) is known to 'B' there is no need of sending (kG).Hence the point ($Pm+kP_B$) which is Pc (Cipher text) is sent to is sent to 'B'.
7. 'B' uses its private key nB to decrypt 'Pc' into 'Pm'.

$Pm+kP_B-n_BkG = Pm+k(n_BG) -n_BkG = Pm$

8. This point Pm is decoded into message.

4. DISCRETE WAVELET TRANSFORMS

A wavelet is an oscillation which exists for short duration and is characterized to have amplitude and frequency ranging from low to high. Usually amplitude starts at zero, increases and then decreases and returns to zero . Figure 2 shows an example of wavelet. Wavelets can be combined, using a convolution, with portions of a known signal to extract information from the unknown signal. A wavelet can be defined in three ways [19]:

Table 1: Generation of Private and Public keys

	A	B
Select private key	$n_A<n$	$n_B<n$
Generate Public key	$P_A=n_AxG$	$P_B=n_Bx G$

a. Scaling filter [g]: Here the high pass filter is the quadrature mirror filter of the low pass, and reconstruction filters are the time reverse of the decomposition filters (Daubechies and Symlet wavelets)
b. Scaling function [φ(t)]: Equivalent to the scaling filter g with finite length(Meyer wavelets).
c. Wavelet function [ψ(t)]: a band-pass filter having a time domain representation and scaling it for each level halves its bandwidth. Hence requires infinite level decomposition to cover the entire spectrum (Mexican hat wavelets)

The representation of such a function by wavelets is called wavelet transform i.e. the daughter wavelets are scaled and translated copies of a finite-length or fast-decaying oscillating mother wavelet or analyzing wavelet. Wavelet transforms are more advantageous than Fourier transforms for representing functions that have discontinuities and sharp peaks, and for deconstructing and reconstructing finite, non-periodic and/or non-stationary signals.

Wavelet algorithms process data at different scales or resolutions. Temporal analysis is performed with a contracted, high-frequency version of the mother wavelet. Frequency analysis is performed with a dilated, low-frequency version of the same wavelet. Therefore original signal is its wavelet expansion (using coefficients in a linear combination of the wavelet functions) and thus data operations are performed using corresponding wavelet coefficients making wavelets an excellent tool in the field of digital signal and image processing.

In discrete wavelet transform (DWT) wavelets are discretely sampled which captures both frequency and location information (location in time). In DWT the mother wavelet is shifted and scaled by powers of two:

$$\Psi_{j,k}(t) = \frac{1}{\sqrt{2^j}}\Psi\left(\frac{t-k2^j}{2^j}\right)$$

where j → scale parameter , k → shift parameter, both which are integers.

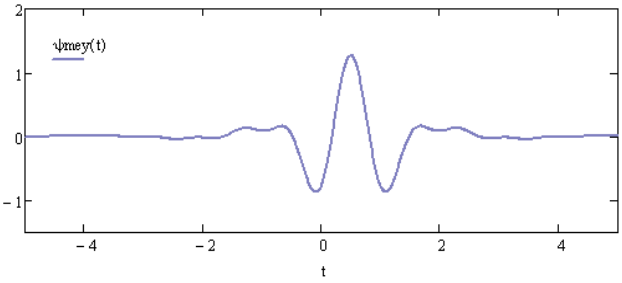

Figure 2 Meyer Wavelet [18]

Figure 3 One level decomposition [19]

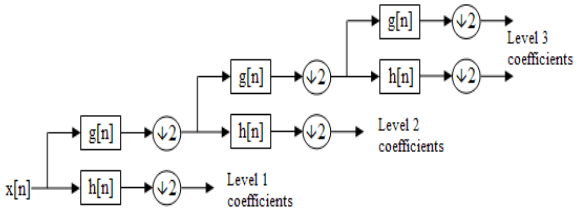

Figure 4 Three level Filter bank [19]

Figure 3 shows the one order filter analysis and the corresponding output equations are given by,

$$y_{low}[n] = (x * g) \downarrow 2 = \left(\sum_{k=-\infty}^{\infty} x[k]g[2n-k]\right) \downarrow 2$$

$$y_{high}[n] = (x * h) \downarrow 2 = \left(\sum_{k=-\infty}^{\infty} x[k]h[2n-k]\right) \downarrow 2$$

Figure 4 shows the three level filter analysis. Haar transform is the first known wavelet which is non continuous and hence non differentiable used as countable orthonormal system for the space of square integral functions on the real line.

The Haar wavelet's mother wavelet function

$$\Psi(t) = \begin{cases} 1, & 0 \le t < 0.5 \\ -1, & 0.5 \le t < 1 \\ 0, & \text{Otherwise} \end{cases}$$

and its scaling function

$$\emptyset(t) = \begin{cases} 1, & 0 \le t < 1 \\ 0, & \text{Otherwise} \end{cases}$$

The Haar wavelet operates on data by calculating the sums and differences of adjacent elements. The Haar wavelet operates first on adjacent horizontal elements and then on adjacent vertical elements. The Haar transform is computed using:

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

5. DWT OF AN IMAGE [20, 24]

The wavelet transform are multi-resolution in nature and suitable for applications where scalability and tolerable degradation are vital. Hence wavelet transform has widespread acceptance in signal processing and image compression. JPEG-2000 is based upon DWT. Wavelet transform decomposes a signal into a set of basis functions called wavelets obtained by dilations and shifting of mother wavelet:

$$\Psi_{a,b}(t) = \frac{1}{\sqrt{aj}}\Psi\left(\frac{t-b}{a}\right)$$

where a →scaling parameter and b → shifting parameter

The wavelet transform is computed separately for different segments of the time-domain signal at different frequencies. It is designed to give good time resolution and poor frequency resolution at high frequencies and good frequency resolution and poor time resolution at low frequencies. Such transformation is applied recursively on the low-pass series until the desired number of iterations is reached.

The DWT of the cover image obtained using an Analysis Filter pair. First, the low pass filter (LPF) followed by sub-sampling (by 2) is applied to each row of data to separate out the low frequency components of the row. Since the LPF is a half band filter output has half the original number of samples. Similarly the high pass components are separated using HPF and placed by the side of the low pass components. This procedure is done for all rows. This is repeated along column-wise. The resulting two dimensional array of coefficients contains four bands of data, each labelled as LL (Low-Low), HL (High-Low), LH (Low-High) and RH (High-High). This is the first level decomposition. Figure-5 shows the three level pyramidal decomposition of image. Coefficients obtained include an approximation and three detail transform coefficients.

$$A_L f(x,y) = < f(x,y), \emptyset(x,y) >$$
$$D_L^V f(x,y) = < f(x,y), \Psi_L^V(x,y) >$$
$$D_L^H f(x,y) = < f(x,y), \Psi_L^H(x,y) >$$
$$D_L^D f(x,y) = < f(x,y), \Psi_L^D(x,y) >$$

The approximation region has more details of image and if the embedding is done in this region there will be degradation of the image. Hence the embedding is done in other detail co-efficient regions (LH, HL or HH). In the second level decomposition the LL band is decomposed producing even more sub-bands. This can be continued by decomposing in a pyramidal fashion as in figure. Since the colour image has R-,G- and B plane, DWT is applied to each plane separately.

6. LINEAR FEEDBACK SHIFT REGISTER (LFSR)

A single bit random number generator [22] produces 0 or 1. The efficient implementation is to use an LFSR [23] which is based on the recurrence equation:

$$x_n = a_1 \bullet x_{n-1} \oplus a_2 \bullet x_{n-2} \oplus \text{------} \oplus a_m \bullet x_{n-m}$$

Here,

- x_n → ith number generated
- a_i → pre-determined constant[0 or 1]
- ● →AND operator
- ⊕→ XOR operator

Equation implies that a new number (x_n) utilizing m (x_{n-1} ,x_{n-2} ----x_{n-m}) through a sequence of AND-XOR operations. Generated pattern will repeat itself after a certain period which is 2^m -1 in an LFSR. To achieve the maximum period, most a_i s are 0, and only two to four of them are 1. So, actual recurrence equation is fairly simple and different for different values of m.

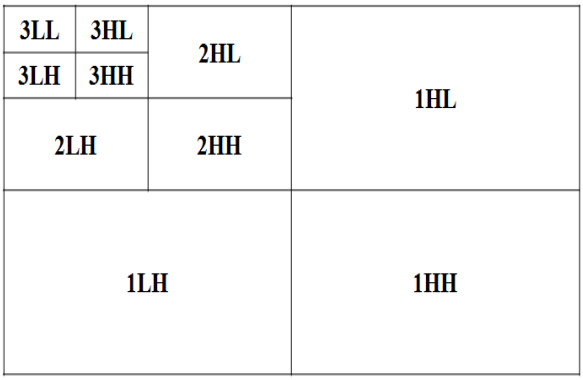

Figure 5 Three level pyramidal decomposition

Leap-forward LFSR method utilizes only one LFSR and shifts out several bits. This method is based on the observation that an LFSR is a linear system and the register state can be written in vector format:

$$q(i+1) = A \bullet q(i)$$

Here, **q**(i +1) and **q**(i) → content of shift register at (i+1)th and ithsteps,**A**→the transition matrix. After the LFSR advances k steps, the equation becomes

$$q(i+1) = A^K \bullet q(i)$$

Let the 4-bit LFSR with

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

$$\therefore \mathbf{A}^4 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

Therefore, $Q_{next} = \mathbf{A}^4 \bullet Q_{present}$

$$q_{0\_next} = q_0 \oplus q_3$$
$$q_{1\_next} = q_0 \oplus q_1 \oplus q_3$$
$$q_{2\_next} = q_0 \oplus q_1 \oplus q_2 \oplus q_3$$
$$q_{3\_next} = q_0 \oplus q_1 \oplus q_2$$

This is realized as shown in Figure 6.

7. PROPOSED SYSTEM AND EXECUTION

The bird view of the proposed method is shown in the Figure 7. The proposed method is a combination of cryptography and steganography done in three stages:

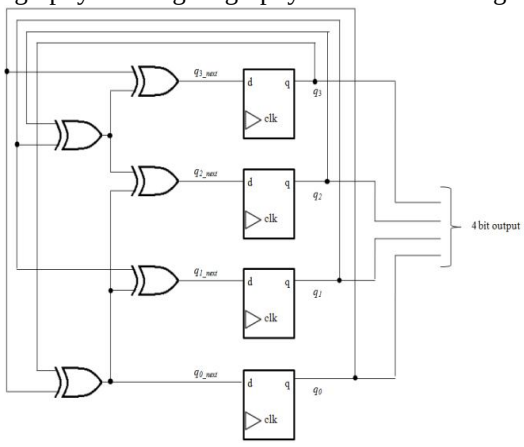

Figure 6 Four-bit Leap-forward LFSR

Stage-1: LFSR Based Passcode generation

The first 4-bits of 163-bits ECC key is used as seed for the 4-bit LFSR . The LFSR iterates 4 times to produce a 16-bit passcode. This 16-bits passcode is used for choosing type of wave filters, level of decomposition, order of detailed regions for embedding using triple stegging. Usage of 16-bits passcode is as follows:

- 1st to 7th bit: since there are 126 types of wavelet filters. 7 bits are dedicated to choose one of wavelet filter. Example- All 7-bits '0' chooses 'db1' Daubechies wavelet filter, similarly all '1' chooses 'rbio6.8' Reverse Biorthogonal wavelet filter.
- 8th -9th bit: These bits together choose the type of filter (low pass, high pass, decomposition or construction) in wavelet filter. The mode of selection is summarized in Table 2.

Table 2: Mode of filter selection

8th-9th bit	Filter Type
00	Decomposition filters
01	Reconstruction filters
10	Low-pass filters
11	High-pass filters

- 10th bit: This bit chooses the number of level of decomposition needed. Bit '0' implicates the one level decomposition. Bit '1'implicates 2- level decomposition of DWT.
- 11th -13th: These bits set the signal or image extension mode for discrete wavelet and wavelet packet transforms. The extension modes represent different ways of handling the problem of border distortion in signal and image analysis. Table 3 summarizes the type of border distortion handling type.
- 14th-16th: used to opt between the 3 coefficients as per the table 4. Example if the passcode is 011 then encrypted data is embedded in second region and this embedded detail is embedded into first region and the embedded details is further embedded on third region and so on.

Table 3: Mode of DWT Extension Mode

11th - 13th	DWT Extension Mode
000	Symmetric-padding (half-point)
001	Symmetric-padding (whole-point)
010	Antisymmetric-padding (half-point)
011	Antisymmetric-padding (whole-point)
100	Zero-padding
101	Smooth-padding of order 1
110	Smooth-padding of order 0
111	Periodic-padding

Table 4: Order of selection of regions for embedding

Passcode	**Order**
001	LH → HL → HH
010	LH → HH → HL

011	HL → LH → HH
100	HL → HH → LH
101	HH → HL → LH
110	HH → LH → HL

Stage-2: Encryption using ECC Algorithm

In this stage, the secret data is encrypted using the public key in ECC algorithm (as explained in section-II).The encryption is shown in the Figure 10.

Stage-3: Embedding using Triple Stegging

The encrypted data in the binary form is embedded into the cover image (Figure 8) and hides its existence. Here a colour image is used as the cover image. The cover image is decomposed by 2-Dimensional Discrete Wavelet Transform (2-DWT) by using Haar's wavelet [6]. This transform provides one approximation and three detail coefficients (horizontal, vertical and diagonal) on each decomposition level (Figure 9). In order to increase the security of the embedded data, the level of decomposition can be increased to any level. But this makes the process more time consuming and tedious. Hence in this method, there is only one level of decomposing at the same time the security is increased by using the concept of Triple-stegging. This method consists of basically three steps (Figure 11):

Step-I : Steganography is once applied to the cover image to embed the encrypted secret data (cipher text) to one area of the detail coefficients(say HL) to obtain the stegoimage.

Step-2: Steganography is applied again to embed that detail coefficient into second detail coefficient region (say LH).

Step-3: Steganography is applied third time to embed that second detail coefficient into third region (say HH)

Figure 12 shown the complete stego image.

Table 5 shows the PSNR value calculated for different amount of embedding. Results summarized here is for db1 decomposition wavelet filter with one level decomposition and order for embedding to be LH → HH → HL.

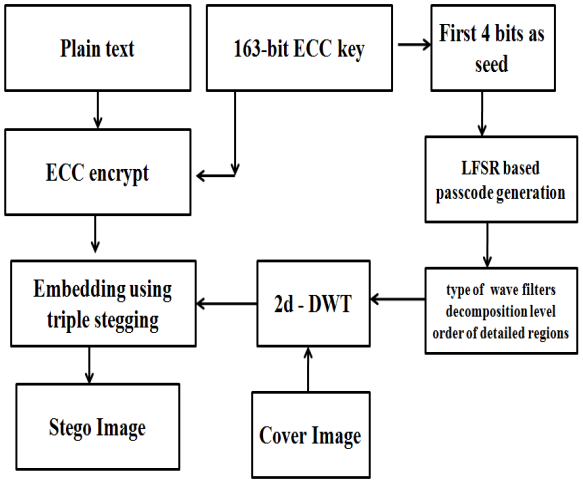

Figure 7 General Block diagram of proposed method

Figure 8 Input image used for Triple stegging

Table 5: PSNR

No of letters	PSNR(dB)
100	140.57
500	140.5584
1000	140.5526
10000	140.3222

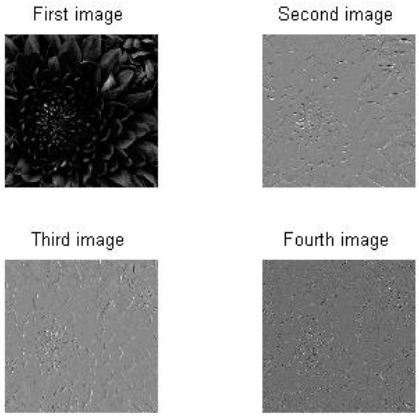

Figure 9 Figure showing low-low, high-low, low-high, high-high frequency components respectively

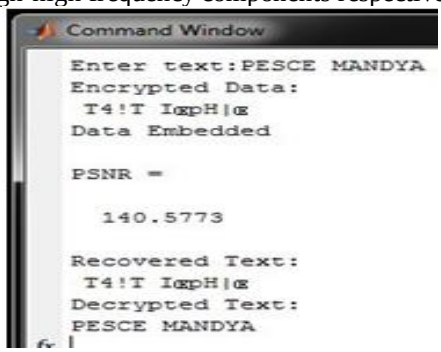

Figure 10 Text converted into Cipher text by making use ECC Algorithm

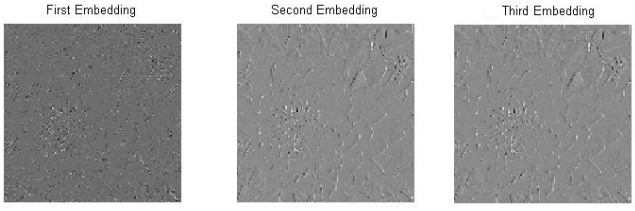

Figure 11 Cipher text Triple stegged into image's

Figure 12 Triple stegged stego image

4. CONCLUSIONS

This method has offered a good visual quality of the coloured stego-image.
Passcode will be architecture based rather than the user based making the architecture more robust against the eavesdropping.
The architecture is dynamic since there is option in choosing type of wave filters, level of decomposition, order of detailed regions for embedding using triple stegging. The flexibility is architecture provides variety in implementation to attain desired robustness and fault tolerance.
Capacity is represented by 1/4 of cover image size for one-level decomposition of the cover image.
Since the cover image is colour image, the embedding capacity will hike to thrice than that of grayscale image. The payload is 0.25 bit/pixel while using the maximum capacity.
Triple Stegging has increased the data security since one coefficient carries the data and the embedding is done thrice even in one level of decomposition. Results infer that Triple stegging has increased PSNR.
In this paper the passcode generation block static i.e., only LFSR method is providing the randomness. In future the passcode generation block can be made dynamic by using multiple methods of random generation like chaotic based, logistic based etc.

REFERENCES

[1]. Committee on National Security Systems: National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, 26 April 2010.
[2]. William Stallings, Cryptography and Network Security Principles and Practices, Fourth Edition, Printice Hall, 2005.
[3]. Behrouz. A. Forouzan, Cryptography and Network Security, Special Indian Edition, Tata Mc-Graw Hill, 2007.
[4]. Whitfield Diffie and Martin E. Hellman, "New Directions in Cryptography", IEEE International Symposium on Information Theory, Ronneby, Sweden, 1976.
[5]. Mulcahy, colm, “Plotting and scheming with wavelets”, Mathematics magazine 69, 5, (1996), 323-343
[6]. Colm Mulcahy Ph. D, "Image Compression using Haar Wavelet Transform", Spelman Science and Math Journal, 22-31.
[7]. Nadiya P v, B Mohammed lmran, “Image Steganography in DWT Domain using Double-stegging with RSA Encryption”, International Conference on Signal Processing, Image Processing and Pattern Recognition [ICSIPR], IEEE, 2013.
[8]. F. Rodriguez-Henriquez, N. A. Saqib, A. D. Pérez, and C. K. Koc, “Cryptographic Algorithms on Reconfigurable Hardware”, New York: Springer-Verlag, 2006.
[9]. Domenico Bloisi and Luca Iocchi, “Image Based Steganography and Cryptography”, Sapienza University of Rome, Italy.
[10]. Dipti Kapoor Sarmah, Neha bajpai, “ Proposed System for Data Hhiding Using Cryptography and Steganography”, International Journal of Computer Applications (0975 – 8887), Volume 8 – No. 9, October 2010.
[11]. Md. Wahedul Islam, Saif alZahir “A Novel QR Code Guided Image Stenographic Technique,” International Conference on Consumer Electronics (ICCE), 2013.
[12]. Konheim, A. Cryptography: A Primer. New York: Wiley, 1981.
[13]. Yadollah Eslami, Ali Sheikholeslami, P. Glenn Gulak, Shoichi Masui, and Kenji Mukaida, “An Area-Efficient Universal Cryptography Processor for Smart Cards”, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 14, PP. 43-56, January 2006.
[14]. Lejla Batina, Nele Mentens, Kazuo Sakiyama, Bart Preneel, Ingrid Verbauwhede “A Low-Cost Elliptic curve cryptography for Wireless sensor networks” ,Springer-Verlag Berlin Heidelberg, 2006.
[15]. Quing Chang, Yong-ping ZHANG, Lin-lin Qin,” A Node Authentication Protocol based on ECC in WSN”, IEEE, 978-1-4244-7164-5.2010.
[16]. Pritam Gajkumar Shah, XuHuang, Dharmendra Sharma, “Analytical study of implementation issues of Elliptical Curve Cryptography for Wireless sensor networks”, IEEE 978-0-7695-4019-1/10.2010.
[17]. A.C.Nuthan, M.S.Naveen Kumar, Shivanand S Gornale and Basavanna, “Development of Randomized Hybrid cryptosytem using Public and Private Keys”, Lecture notes in electrical engineering 248, Emerging Research in Electronics, Computer Science and Technology, Springer India, 2014.
[18]. F. G. Meyer and R. R. Coifman, Applied and Computational Harmonic Analysis, 4:147, 1997.
[19]. Hazewinkel, Michiel, ed., “Wavelet analysis”, Encyclopaedia of Mathematics, Springer, ISBN 978-1-55608-010-4, 2001.
[20]. Ali Al-Ataby and Fawzi Al-Naima, “A Modified High Capacity Image Steganography Technique

Based on Wavelet Transform", The International Arab Journal of Information Technology - IAHT , Vol. 7, No. 4,P g. 358- 364, 2010.

[21]. Shivanand S Gornale and A.C.Nuthan, "Discrete Wavelet Transform (DWT) Based Triple-Stegging with Elliptic Curve Cryptography (ECC)" , International conference on recent trends in Signal Processing, Image Processing and VLSI [ICrtSIV], Research publishing publications, India, 2015.

[22]. P. H. Bardell, W. H. McAnney and J. Savir, "Build-in Test for VLSI: Pseudo-random Techniques", John Wiley and Sons, 1987.

[23]. P. Alfke, "Efficient Shift Registers, LFSR Counters, and Long Pseudo-Random Sequence Generators", Xilinx Application Note, 1995.

[24]. S. S. Gornale and K.V.Kale, "Development of Compression technique for Noisy Image: A Multi-Wavelet approach", Ph.D. thesis University of Pune, Pune-2008

AUTHOR

Dr. Shivanand S Gornale completed M. Sc. in Computer Science. M.Phil. in Computer Science., Ph.D. in Computer Science from University of Pune, in 2009 under the guidance of Dr. K V Kale and has been recognized as research guide for Ph.D. in Computer Science and Engineering from Rani Channamma University, Belagavi and Jain University Bangalore. He has published more than 60 research papers in various National and International Journals and conferences. He is an editorial member for International Journal on Computer Science and IT, International Journal Bioinformatics and Soft Computing (IJBSC), International Journal of Computer Science and Application and also working as reviewer for various International and National Journals and Conferences and also worked as National/International Conferences and Workshops Technical Committee Member.

Dr. S. S. Gornale is a Fellow of IETE New Delhi, Life Member of CSI, Life Member of Indian Unit of Pattern Recognition and Artificial Intelligence (IPRA), Member of Indian Association for Research in Computer Science (IARCS), Tata Institute of Fundamental Research (TIFR), Mumbai, Member of International Association of Computer Science and Information Technology (IACS&IT) Singapore, Member of International Association for Engineers', Hong Kong, Member of Computer Science Teachers' Association, USA and Graduate Member of IEEE, Life Member of Indian Science Congress Association, Kolkata-India. Presently he is working as Associate Professor, Department of Computer Science, Rani Channamma University, Belagavi - Karnataka.

Dr. S. S. Gornale has been nominated as a Best teacher award at university of Pune for the year 2007-2008 and has been also awarded Vidyabhushan" in 2010, by INSA (Indian NET□SET Association, Amravati), Maharashtra-India. His areas of research interest are Biometrics, Image Processing and Pattern Recognition and Information Communication Technology (ICT). He also delivered invited talks/as a Session Chair at various national conferences and workshops. He has been serving as a resource person for UGC academic staff colleges in University of Mysore, Karnataka University, Dharwad, Dr. BAMU, Aurangabd-Maharashtra and Administrative Training Institute (ATI), Mysore.

Nuthan A. C completed B.E. and M. Tech in Electronics and Communication Engineering. Presently he is working as an Associate Professor in Electronics Communication Engineering, Department of ECE, GMIT, Bharathinagara, Karnataka, India. Presently he is pursuing his Ph.D. in Electronics and Communication Engineering from Jain University, Bangalore.