Randomized Passcode Generation For Triple-Stegging Using DWT And ECC

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

[1] **Department of Computer. Science, Rani Channamma University,Belagavi, Karnataka,India.**

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

Abstract

Preserving sensitive information is an greatest challenge in this communication world. Information security has higher prominence in any organization. The paper works for such security by embedding sensitive data in color images. In this proposed technique Cryptography and Steganography both work together to have an increased security level. Encrypted data (using cryptography) is embedded into an image (cover media) using Triple- Stegging. The 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 [18]. The sensitive data to be stored and transmitted is converted to unrecognizable form using cryptography and steganography [9-11].

In cryptography plaintext (text, image, audio, video) is converted to ciphertext using encryption algorithm and a key [20,21,29]. The reverse of data encryption is data Decryption. Private 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.

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 using stego system encoder and secret key. The resulting stego image is then transmitted or stored. During retrieval of data, the stego decoder gives an estimate of the secret data.

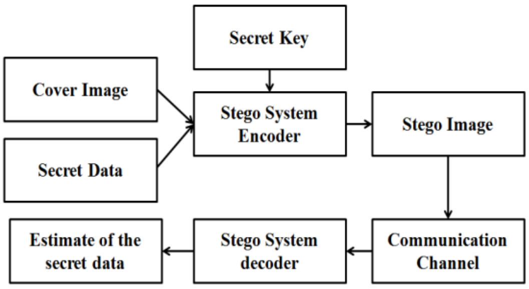


Figure 1: Typical steganography system

2. Problem Formulation

The advantage of Public Key cryptography over Private key cryptography is the sender is avoided to share secret key with the receiver. Hence public key cryptography like ECC ,RSA is be preferred. ECC gives a higher security level than RSA with smaller key size [10]. ECC is used which is dealt in Section III.

The non-recognizable form of cipher text confirms a hacker with the existence of secret data. To hide the existence of ciphered data, the cryptography stage is followed by steganography to embed the ciphered data into cover image. Hence the architecture comprises the both to cryptography and steganography to hike the security level. The cover image could be gray scale image [28] or colour image [31].

The embedding is done by modifying the detail coefficients in transform domain of Two-Dimensional Discrete Wavelet Transform (DWT). This enables large data capacity and good visual quality of the stego image and suppresses the energy compaction of secret data. This paper uses DWT approach for embedding the secret data which is dealt in Section IV and Section V. DWT presented uses abstract mathematical setting using special function in [5,28]. Matrix multiplication produces smoother and satisfactory compressed images [19]. Since the nature of image is also matrix, DWT is implemented using matrix multiplication approach as in [31,32].

The DWT is followed by Triple Stegging technique to increase the security level of data. A similar work has been carried out using RSA algorithm and double-stegging [28] and RSA algorithm and Triple-stegging [32].

Selection of detailed coefficient regions (LH,HL,HH) in DWT is static in [28] i.e., the two regions say HH and HL are selected for embedding the data, then the same regions are retained in all data transaction and there was no flexibility to select other regions in future data transaction. In [31] the architecture was made flexible to select the detailed coefficient regions. 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 not non-generative i.e. it should be given externally. As an improvisation, in paper [8] the 3-bit passcode is generated by the passcode generation block in the architecture and hence the user himself will not know the passcode to choose the 3 regions.

In [31], only one wavelet filter was used in the architecture. In [32] the architecture is pliable to choose one among 126 wavelet filters. The choice of the wavelet filter is by 7-bits in the passcode. The same is used in this paper.

In [31] the architecture handled one-level decomposition in DWT. The paper [32] can undertake one or two level decomposition based on passcode. The same is used in this paper.

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. The Paper [31] does not handle border distortion. The paper [32] handles border distortion efficiently with the mode flexibility based on the passcode.

These enhancements to the previous work [5, 28,31] recommends integration of Passcode generation block in the architecture. Hence LFSR based Passcode generation block [32] generates 16-bit passcode which makes the architecture flexible in choosing type of wave filters, level of decomposition, order of detailed regions for embedding using triple stegging. In order to enhance the randomness further, 4 types of random generators are used in this paper instead of single LFSR technique [32]. A 2-bit seed is used to select one of the random number generators at time of data transaction. Hence there is randomness in choosing the random number generator.

3. Elliptic Curve Cryptography [2,11,12,22,23,30]

Public key cryptography ECC, suggested by Neil Koblitz and Victor. S, 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 defined by a cubic equation of the form:

$$y^2 = x^3 + ax + b \quad \text{with} \quad 4a^3+27b^2 \neq 0. \qquad (1)$$

Table 1: Generation of Private and Public keys

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

Steps to perform the ECC encryption and decryption:

1. Select an Elliptic Curve 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 mod p= x^3 + ax + b mod 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 pointG ∈ 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’.
   $$P_C=[(kG),(Pm+kP_B)] \qquad (2)$$
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’.
   $$Pm+kP_B-n_BkG = Pm+k(n_BG) - n_BkG = Pm \qquad (3)$$
8. This point Pm is decoded into message.

4. Discrete Wavelet Transforms (DWT)

A wavelet is a short duration oscillation having amplitude and frequency ranging from low to high. 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. 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.

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:

$$\Psi_{j,k}(t) = \frac{1}{\sqrt{2^j}}\Psi\left(\frac{t-k2^j}{2^j}\right) \qquad (4)$$

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

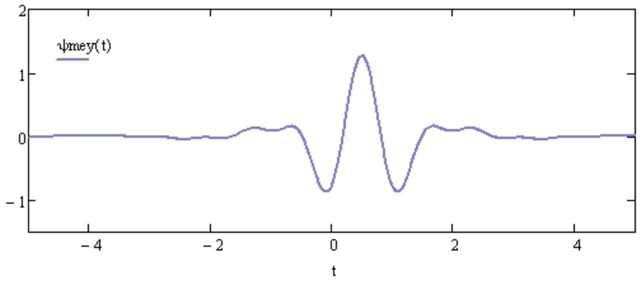


Figure 2: Meyer Wavelet [6]

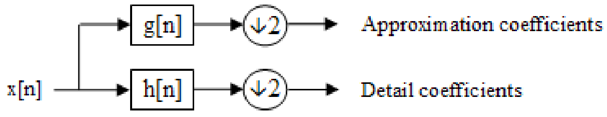


Figure 3: One level decomposition [7]

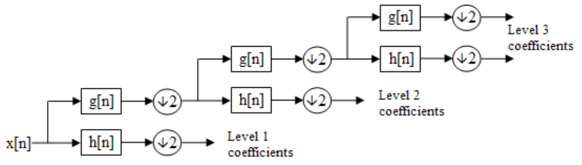


Figure 4: Three level Filter bank [7]

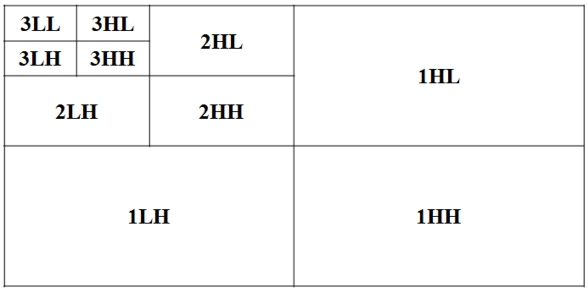


Figure 5: Three level pyramidal decomposition

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

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

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

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

$$\Psi(t) = \begin{cases} 1, & 0 \le t < 0.5 \\ -1, & 0.5 \le t < 1 \\ 0, & \text{Otherwise} \end{cases} \quad (7)$$

and its scaling function

$$\emptyset(t) = \begin{cases} 1, & 0 \le t < 1 \\ 0, & \text{Otherwise} \end{cases} \quad (8)$$

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:

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (9)$$

5. DWT Of An Image [20]

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 if the image shown in the figure 5. Coefficients obtained include an approximation and three detail transform coefficients.

$$A_L f(x,y) =< f(x,y), \emptyset(x,y) > \quad (10)$$

$$D_L^V f(x,y) =< f(x,y), \Psi_L^V(x,y) > \quad (11)$$

$$D_L^H f(x,y) =< f(x,y), \Psi_L^H(x,y) > \quad (12)$$

$$D_L^D f(x,y) =< f(x,y), \Psi_L^D(x,y) > \quad (13)$$

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. Random Number Generator

Random numbers are used in a data encryption, circuit testing, system simulation and Monte Carlo method. The software-based methods of the random number generation require complex arithmetic operations and thus to make digital systems faster and denser random number generators are directly implemented in hardware. This paper uses 4 random number generators .

A. Linear Feedback Shift Register (LFSR) [4]

A single bit random number generator [3] produces 0 or 1. The efficient implementation is to use an LFSR [4] which is based on the recurrence equation:

$$x_n = a_1 \bullet x_{n-1} \oplus a_2 \bullet x_{n-2} \oplus\text{------}\oplus a_m \bullet x_{n-m} \quad (14)$$

Here, x_n→ ith number generated, a_i→ pre-determined constant[0 or 1], • →AND operator, ⊕→ XOR operator . Generated pattern will repeat itself after a certain period which is 2^m -1 in an LFSR.

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:

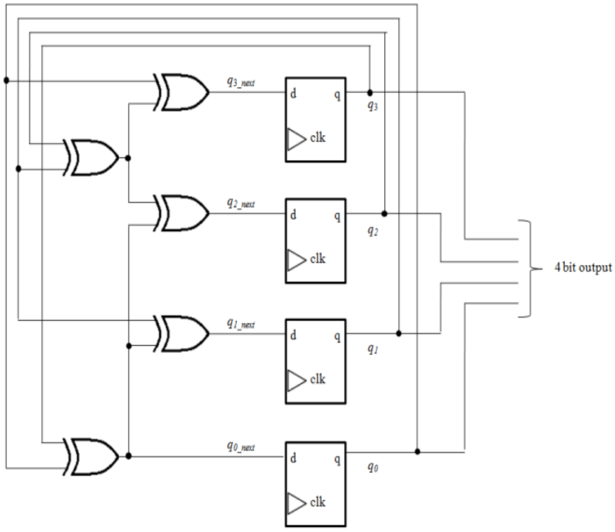


Figure 6: Four-bit Leap-forward LFSR

$$q(i+1) = A \bullet q(i) \quad (15)$$

$$q(i+1) = A^K \bullet q(i)$$
(16)

Let the 4-bit LFSR with

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} \quad (17)$$

$$\therefore \mathbf{A}^4 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \quad (18)$$

Therefore, $Q_{next} = \mathbf{A}^4 \bullet Q_{present}$ (19)

$$q_{0\_next} = q_0 \oplus q_3 \quad (20)$$
$$q_{1\_next} = q_0 \oplus q_1 \oplus q_3 \quad (21)$$
$$q_{2\_next} = q_0 \oplus q_1 \oplus q_2 \oplus q_3 \quad (22)$$
$$q_{3\_next} = q_0 \oplus q_1 \oplus q_2 \quad (23)$$

This is realized as shown in Figure 6.

B. Chaos-based random number generator [8,16,25,15,26]

Chaos-based encryptions spread the initial region over the entire phase space, but cryptographic algorithms shuffle and diffuse data by rounds of encryption [8]. Therefore, the security of chaos-based encryptions is defined on real numbers through mathematical models of nonlinear dynamics while conventional encryption operations are defined on finite sets. Most existing chaos-based encryptions based on such two-stage operations employ both initial conditions and control parameters of I-D, 2-D, and 3-D chaotic maps such as Baker map [16], Arnold cat map [25], and Standard map [15] for secret key generations. Furthermore, the combinations of two or three different maps have been suggested [26,17] in order to achieve higher security levels. The chaotic function that is used is given by

$x(i+ 1) = \mu x(i)(1-x(i))$ (24)

Where $\mu=3.9$.

C. BB (Brahmagupta-Bhaskara) equation based random number generator [13]

The BB equation in galois field G(p) is written as

$$|n(x^2)_p|_{p+1} = (y^2)_p \quad (25)$$

Where p is an odd prime.

D. Compound Sine and Cosine Chaotic Maps [27]

Sine and cosine maps offers rich dynamic behaviors [2] and high complexity in terms of nonlinear dynamics,

(16)Here, **q**(i +1) and **q**(i) → content of shift register at (i+1)th and iths

$X_{n+1}=\sin(ax_n)$ and $X_{n+1}=\cos(bx_n)$ (26)

where a and b are frequencies parameters of sine and cosine functions, respectively. As an enhancement a combination between sine and cosine maps is used, i.e.

$$x_{n+1} = \cos(ax_n) + \sin(bx_n) \quad (27)$$

This combinations offers high-degree of chaos over most regions of parameter spaces. The initial conditions and control parameters can be used as internal security keys.

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:

Stage-1: Randomised Passcode generation

The first 2-bits of 163-bits ECC key is used to select one of the 4 types of random number generators. Table 2 gives the selection of type of random number generation. The next 4-bits of 163-bits ECC key is used as seed for the 4-bit random generator. This random number generator produces a 16-bit passcode. This 16-bits passcode is used to choose 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: 7 bits are dedicated to choose one of 126 types of wavelet filters. 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 (lowpass, highpass ,decomposition or

construction) in wavelet filter. The mode of selection is summarized in Table 3.

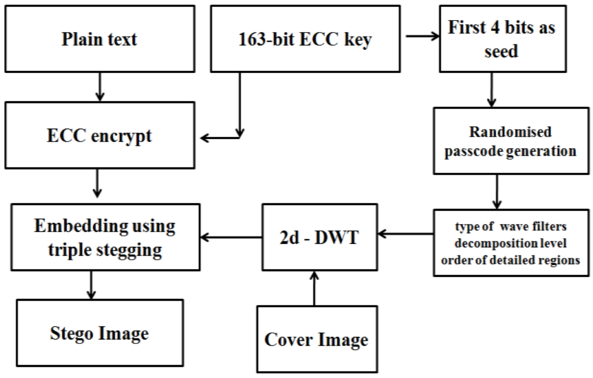

Plain text
163-bit ECC key
First 4 bits as seed
ECC encrypt
Randomised passcode generation
Embedding using triple stegging
2d - DWT
type of wave filters decomposition level order of detailed regions
Stego Image
Cover Image

Figure 7: General Block diagram of proposed method

Table 2: Mode of random number generation

First 2 bits of 163 bit ECC key	Random Number generation type
00	Linear Feedback Shift Register (LFSR)
01	Chaos-based random number generator
10	BB equation based random number generator
11	Compound Sine and Cosine Chaotic Maps

Table 3: Mode of filter selection

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

Table 4: 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 5: 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

- 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 4 summarizes the type of border distortion handling type.
- 14th-16th: used to opt between the 3 coefficients as per the table 5. 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.

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 [19]. 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 either one or two level of decomposition. This method consists of basically three steps (Figure 11):

Step-l : 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 6 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.

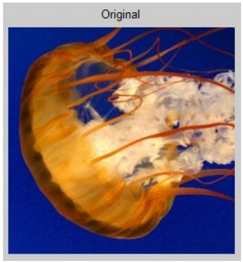


Figure 8: Input image used for Triple stegging

Table 6: PSNR

No of letters	PSNR(dB)
100	146.57
500	146.5584
1000	146.5526
10000	146.3222

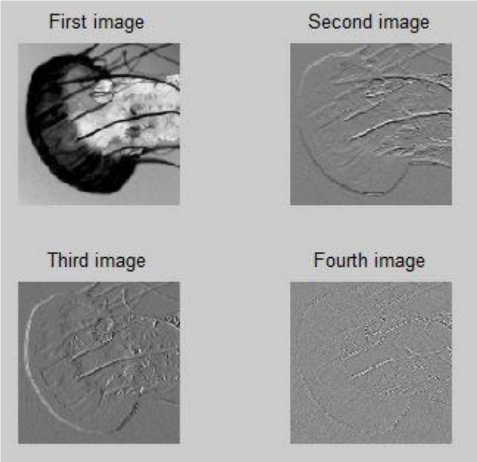
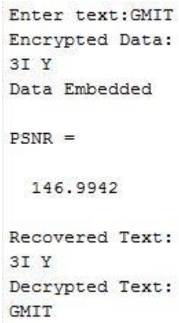


Figure 9: Figure showing low-low, high-low, low-high, high-high frequency components respectively



```
Enter text:GMIT
Encrypted Data:
3I Y
Data Embedded

PSNR =

  146.9942

Recovered Text:
3I Y
Decrypted Text:
GMIT
```

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

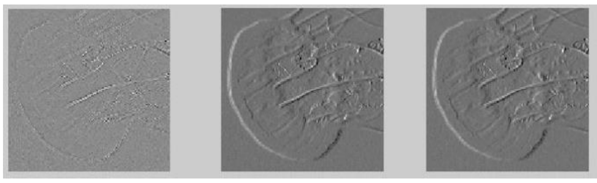


Figure 11: Cipher text Triple stegged into image's

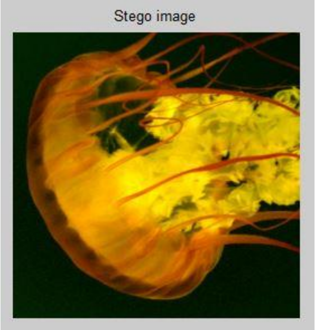


Figure 12: Triple stegged stego image

8. 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 the passcode generation block is made dynamic by using multiple methods of random generation like chaotic based, logistic based etc.

REFERENCES

[1] Whitfield Diffie and Martin E. Hellman, "New Directions in Cryptography", *IEEE International Symposium on Information Theory*, Ronneby, Sweden, 1976.

[2] Konheim, *A. Cryptography: A Primer*. New York: Wiley, 1981.

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

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

[5] Mulcahy, colm, “Plotting and scheming with wavelets”, *Mathematics magazine* 69, 5, (1996), 323-34.

[6] F. G. Meyer and R. R. Coifman, *Applied and Computational Harmonic Analysis*, 4:147, 1997.

[7] Hazewinkel, Michiel, ed., “Wavelet analysis”, *Encyclopaedia of Mathematics*, Springer, ISBN 978-1-55608-010-4, 2001.

[8] G. Chen, Y. Mao, CK Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps", Chaos, Solitons and Fractals, Vol. 2 1, pp. 749-761,2004.

[9] William Stallings, *Cryptography and Network Security Principles and Practices*, Fourth Edition, Printice Hall, 2005.

[10]F. Rodriguez-Henriquez, N. A. Saqib, A. D. Pérez, and C. K. Koc, “Cryptographic Algorithms on Reconfigurable Hardware”, New York: Springer-Verlag, 2006.

[11] 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.

[12]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.

[13] N.Rama Murthy and .N.S.Swamy,"Cryptographic Applications of Brahmagupta Bhaskara Equation", IEEE Transactions on circuitS-I, Regular papers, voL53, July2006, pp.I565-I571.

[14] Behrouz. A. Forouzan, *Cryptography and Network Security*, Special Indian Edition, Tata Mc-Graw Hill, 2007.

[15] K. Wong, B. Kwok, and W. Law, "A Fast Image Encryption Scheme based on Chaotic Standard Map", Physics Letters A, Vol. 372, pp. 2645-2652, 2008.

[16] X. Tong, M. Cui, "Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator", Signal Processing, Vol. 89, pp. 480-491, 2009.

[17] F . Huang, Y . Feng, "Security analysis o f image encryption based on two-dimensional chaotic maps and improved algorithm", Front. Electr. Electron. Eng. China, Vol. 4, No. 1, pp. 5-9,2009.

[18] Committee on National Security Systems: *National Information Assurance (IA) Glossary*, CNSS Instruction No. 4009, 26 April 2010.

[19] Colm Mulcahy Ph. D, "Image Compression using Haar Wavelet Transform", *Spelman Science and Math Journal*, 22-31,2010.

[20] Domenico Bloisi and Luca Iocchi, “Image Based Steganography and Cryptography”, Sapienza University of Rome, Italy.2010.

[21] 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.

[22] Quing Chang, Yong-ping ZHANG, Lin-lin Qin,” A Node Authentication Protocol based on ECC in WSN”, *IEEE*, 978-1-4244-7164-5.2010.

[23] 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.

[24] 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.

[25] X. Ma, C. Fu, W. Lei, S. Li, "A Novel Chaos-based Image Encryption Scheme with an Improved Permutation Process", International Journal of Advancements in Computing Technology, Vol. 3, No. 5, 20 1 1.

[26] K. Gupta, S. Silakari, "New Approach for Fast Color Image Encryption Using Chaotic Map", Jour. of Information Security, pp. 139-150,2011.

[27] S. Maksuanpan, T. Veerawadtanapong, w. San-Urn, “Robust Digital Image Cryptosystem Based on Nonlinear Dynamics of Compound Sine and Cosine Chaotic Maps for Private Data Protection”, ISBN 978-89-968650-1-8, ICACT2013, IEEE,2013.

[28]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.

[29] Md. Wahedul Islam, Saif alZahir “A Novel QR Code Guided Image Stenographic Technique,” *International Conference on Consumer Electronics (ICCE)*, 2013.

[30] 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.

[31] 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.

[32] Shivanand S Gornale and A.C.Nuthan, “Self generative passcode for Triple-Stegging using Discrete Wavelet Transform (DWT) and Elliptic Curve Cryptography (ECC)” , *Volume 2, Issue 4,ISSN 2278-6856, International Journal of Emerging Trends & Technology in Computer Science [IJETTCS]*, India, 2015.