VOL. 14, NO. 15, AUGUST 2019 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

ECC ENCRYPTED SECURE REVERSIBLE DATA HIDING ON REAL TIME IMAGES WITH ENHANCED SECURITY

Shima Ramesh Maniyath[1,2] and R. Geetha[1,2]
[1,2]School of Electronics Engineering (SENSE), VIT University, Vellore Campus, India
[1,2]M.V.J. College of Engineering, Bangalore, India
E-Mail: ramesh.shima86@gmail.com

ABSTRACT

Reversible data hiding in encrypted domain (RDHED) has greatly attracted researchers as the original content can be losslessly reconstructed after the embedded data are extracted, while the content owner's privacy remains protected. Connecting the probable feature of public key cryptosystem, the proposed system utilizes elliptical curve cryptography for cost effective computation of secret keys required for performing encryption. Steganography process hides message into cover file and forms a stego file. In image steganography there is a need of method which will increase the security, reduce the distortion in the stego file and recovers the data without any loss. The proposed approach is the combination of data hiding technique and encryption. The image is encrypted using ECC to ensure user authentication. The key which are very confidential can be hidden into an encrypted image which is made a watermark image by applying the RDH (Reversible data hiding algorithm) without changing the bit stream size. Once receiver got encrypted stego file they can access the secret key by using a reverse process of data hiding. ECC is a superior option for open key encryption. It gives parallel security smaller key size.

Keywords: reversible data hiding, ECC.

1. INTRODUCTION

Encryption is a type of security that can be done by using a collection of complex algorithms to the original content meant for encryption by converting data, programs, images or other information into unreadable cipher. Encryption is significant because it permits you to securely protect data that you don't want anyone else to have access to. After Encryption data is jumbled up in a manner so that when it travels through the internet it is completely unreadable, this stops hackers who may intercept the data from seeing what you're doing, as all they'd receive is a random bunch of letters, numbers & symbols. Many individuals use it to protect personal information to guard against things like identity theft. Businesses use it to protect corporate secrets, governments use it to secure classified information, and in cryptography, a key is a piece of information that controls the functional output of a cryptographic algorithm. To prevent a key from being guessed, keys need to be produced truly randomly and contain sufficient entropy. The problem of how to safely generate truly random keys is difficult, and has been addressed in many ways by various cryptographic systems .To plug this security hole, most safe online transactions now use a variant of what is known as asymmetric encryption or public-key encryption. Public-key encryption uses two keys for locking and opening up data: a public key that is shared with anyone, and a private key that stays with the sender of encrypted data. Encryption key management is administering the full lifecycle of cryptographic keys and protecting them from loss or misuse. The lifecycle includes: generating, using, storing, archiving, and deleting of keys. However, in some applications, the transmission of a secret key through a secure channel is unfeasible .Protection of the encryption keys includes limiting access to the keys physically, logically, and through user/role access. In this paper, we present a Reversible data hiding in encrypted signals with public key cryptography. The original image is encrypted by ECC encryption with a public key. After that, the data-hider directly hides the secret key in the encrypted signal with RDH. In our separable framework, there are two separate cases occurring at the receiver side. The receiver who has only the data-hiding key without prior knowledge of the original content can directly extract the embedded data from the received marked encrypted signal. Though, the receiver who has only the private key cannot retrieve the embedded data. But he can directly decrypt the received marked encrypted signal to obtain the original image without loss. The proposed method safeguards that the image decryption and data extraction are independent at the receiver side. Furthermore, compared with the image encrypted with a cipher stream, the proposed scheme is more applicable in the cloud without degrading the security level.

The paper is organized as follows: In Section 2, we discussed about related work .Section 3 described our problem statement. Section 4 described about the proposed methodology (ECC cryptosystem and RDHED scheme), where we also describe the procedures for extracting the embedded data and recovering the original image. The proposed method is experimentally validated in Section 5. Finally, the paper is concluded in Section 6.

2. RELATED WORK

All the prevailing methods gives a technique for hiding a data into an image in a reversible manner while during the extraction phase the image will be restored lossless but the security of an image with hidden data is also a major concern especially during transmission. And

when the image and the data inside it have a relation in that case both the data and image should not be revealed to the unauthorized user. Chen et al. proposed a RDH method with public key cryptosystem for encrypted signal. They used Paillier encryption to embed into adjacent encrypted pixels. Zhang *et al*. proposed a homomorphic property to combine the RDH for images encrypted with public-key cryptosystem. Miss. Nuzhat Ansaria and Prof. Rahila Shaikh has proposed scheme of RDH for hiding data, in that image is encrypted using visual cryptography which involves dividing the image into random shares. After data embedding they modified pixel values of used pixels. Due to this reason there is an ambiguity in the encrypted image. Aswathy Achuthshankar et al proposed an algorithm for reversible data hiding with a novel lightweight software oriented symmetric stream cipher namely A-S algorithm. The performance analysis are done in two phases. They are:

2.1. Encryption algorithm (A-S Algo.) analysis phase

2. Embedding Data Analysis Phase. But the major issue is that embedding data capacity is depend on the cover image that is selected.

3. PROBLEM DESCRIPTION

After revising the existing approaches, it has been explored that chaotic map is primarily used as an image scrambling technique whereas the encryption mechanism discussed is quite complex in its origin. The major hazards is i) large number of steps for encryption with highly computational complexity ii) lack of security for the transmitted key. iii) Trade-off between image quality and security demands, iv) doesn't ensure optimal image imperceptibility. It is also found that there is a less survey of many other standard cryptographic techniques in image encryption process. Therefore, the problem statement is "Building a novel image encryption algorithm with RDH technique to hide the key on encrypted image so that encryption scheme not only offer cost effective but also retains maximum level of image imperceptibility".

4. PROPOSED METHODOLOGY

The execution of the proposed image encryption scheme is carried out considering systematic research methodology. Figure-1 highlights the adopted flow of the proposed system

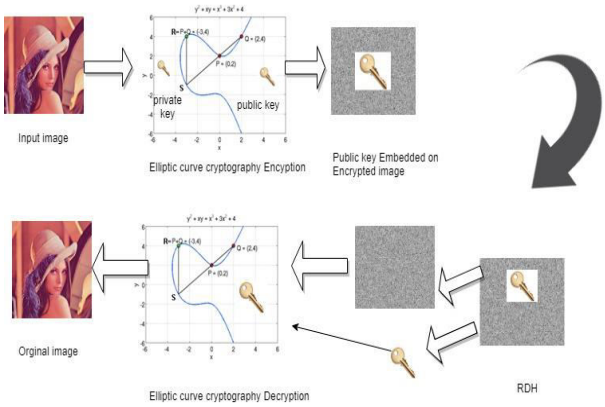


Figure-1. Block diagram of Proposed Methodology.

In recent years, advancement hiked the fear of receiving the data snooped at the time of sending it from the sender to the receiver because of this reason Information Security in the field of digital communication has become more relevant. So, a secure technique is designed to integrate both Cryptography and Steganography. Primarily, user's trustworthy data are encrypted using the more secure Multi curve Elliptic Curve Cryptography (ECC) technique. Next, the secret key used for encryption is embedded into the encrypted image by using a novel proposed Reversible data hiding in encrypted domain (RDHED), a steganography technique to embed the secret data. While embedded encrypted confidential data are transmitted through a channel to the receiver. Finally, the user's secret data is extracted and it is de-ciphered. This proposed technique increases carrier capacity and embedding efficiency when compared to existing methodologies and there by enhances the level of security and robustness against attacks.

4.1 Encryption

The proposed system performs grouping of n-number of pixels followed by calculation of public key using elliptical curve cryptography, which belongs to the first level of Encryption. A point addition is used followed by de-grouping of the pixels and further using DNA Digital coding Technology, three matrices are generated. The scrambling is performed on the first encrypted image followed by bitwise XOR operation with the DNA templates to obtain the finally encrypted image. The next section further illustrates the algorithm implemented for achieving the presented image security goals.

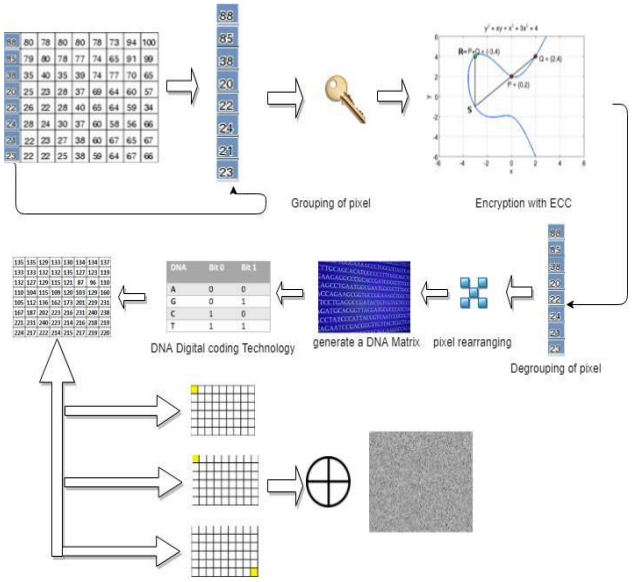


Figure-2. Block diagram of Encryption.

4.2 Algorithm implementation

The proposed algorithm highlights on applying lightweight highly confidential cryptographic operation in order to perform encryption of an image. For this purpose, the algorithm design utilizes elliptical curve cryptography as well as nucleotide sequence coding technology in order to ensure holding of both forward and backward secrecy. The implementation of the algorithm is carried out by dual phases of encryption called as first level and second level of encryption for a given image. Following are the descriptions of algorithms:

i) Algorithm for first level of encryption

This algorithm is responsible for performing principal encryption where implementation of elliptical curve cryptography is mainly used. The algorithm takes the input of r1/r2 (random numbers), P (Private Key), Pb (Public Key), n (value to be embedded) that yields and output of level1_enc (encrypted image). The steps of the algorithm are as follows:

Algorithm for Primary Encryption
Input: r1/r2, P, Pb, n
Output: level1_enc
Start
1. init r1, r2, P, Pb, n
2. For i=1:V
3. INT→f1(val)
4. Pm→[INT]
5. End
6. For j=1:Pm
7. ypm→g(x1, H), where H=a, b, p
8. [CI YCI]→gadd(x1, ypm(j), Kpb, yKpb, H)
9. end
10. For j=1:CI
11. op→f2(CI)
12. Ilevel1_enc →op
13. end
End

The algorithm initiates its execution by defining a random number r1 and r2 for transmitter and receiver (Line-1). This random number r2 is also used for computing public key Pb which is a product of r2 and P. The dimension of the image I is converted to a double precision in order to obtain V followed by adding an extra value to make it multiple of n (Line-2). A function f1 is applied for transforming base to variable precision integer for all the values of V in order to obtain a integer-formed matrix INT (Line-3). All the output of INT is appended in order to obtain Pm (Line-4). The next part of the algorithm is to compute a secret key Kpb that is obtained by product of initial random number r1 with public key Pb. The study also construct a matrix H that reposits the value of three points on elliptical curve i.e. a, b, and p points (Line-7). A function g is applied that represents standard elliptical curve with input arguments of secret key Kpb and matrix H. This is followed by applying a function gadd for representing addition. Point operation on elliptical curve considering input arguments of initial random number x1, the curve ypm, secret key Kpb, ykpb, and H (Line-8). This operation leads to the output of cipher image CI which is further subjected to another inverse function f2 that converts variable precision integer to base value for the cipher text obtained (Line-11). In case the length of this matrix op is found to be less than n than we add zeros. Finally, we obtained first level of encrypted image Ilevel1_enc using elliptical curve cryptography (Line-12). This output is further subjected to secondary encryption process as briefed below.

ii) Algorithm for second level of encryption

This algorithm performs secondary stage of encryption which takes the input as level1_enc (encrypted image) leading to an output of level2_enc (final encrypted image). The steps of the algorithm are as follows:

Input: level1_enc
Output: level2_enc
Start
1. [nr nc]=size(I_c), where I_c→ level1_enc
2. $A_1=S_{img}(I_c, K_{pb})$
3. $D_{mat}\rightarrow f_3(K)$, where K=a, c, t, g
4. $B_1=D_{mat}$, $B_2=D_{mat}$', $B_3=flip(D_{mat})$
5. $A_2=A_1 \oplus B_1$
6. $A_3=A_2 \oplus B_2$
7. $A_4=A_3 \oplus B_3$
8. level2_enc →A_4

end

The first step of this algorithm is to perform reshaping of the primary encrypted image in order to obtain I_c followed by extraction of number of rows *nr* and columns *nc* in it (Line-1). The next step of the algorithm is apply a function S_{img} to perform scrambling operation of encrypted image I_c using a secret key i.e. K_{pb} (Line-2).

This operation results in first matrix A_1.The next step of the algorithm is to generate a nucleotide sequence K where K is a set of elements a, c, t, and g with permutations of different strings (Line-3). A specific function f_3 is applied in order to create the nucleotide sequence in order to generate a matrix D_{mat} (Line-4). The algorithm also generates three different matrix viz. A_1, A_2, and A_3 formed by considering same matrix D_{mat}, transpose of D_{mat} as D_{mat}', and complete 90^o flipping of D_{mat}' matrix respectively followed by performing bitwise XOR operation of obtained A_1 with double precision with image pixel i.e. B_1 in order to obtain A_2 matrix (Line-5). The process continues in order to obtain A_4 (Line-7) which finally results in secondary encrypted image level2_enc as output (Line-8). Therefore, it can be seen that proposed system offers a simplified encryption operation in order to ensure the light weighted feature of ciphering the image. One of the innovative contributions of the proposed system is that owing to its design principle, the proposed algorithm with positively maintains progressively enhanced signal quality in every reconstructed image. The next section discusses outcomes obtained after implementing RDH algorithm on the final encrypted image.

In the proposed method embedding and extraction procedures are described through flow chart in Figure-3.

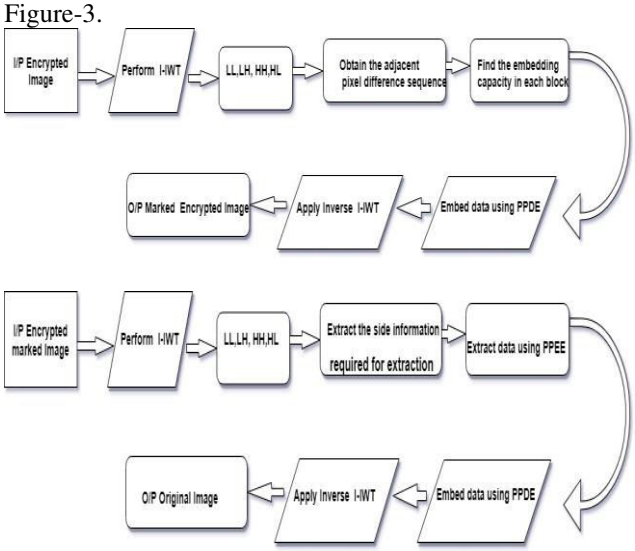


Figure-3. Flow chart for (a) Embedding (b) Extraction.

Embedding Procedure:

a) The input encrypted image is performed an Integer-Integer Wavelet Transformation resulting in the following sub bands: HH, HL, LL, LH

b) Pixel difference of the pair sequence (e1, e2,…eM) is determined in each block by means of prediction.

c) Find the embedding capacity in each block by constructing the histogram of adjacent pixel difference values.

d) Determine the smallest integer ∂ in such a way that you get enough number of pairs to embed the data in the given sub-band.

e) Adjust the pixel value by 1 to avoid overflow/ underflow, note down the locations of the modified pixels and compress the location map(LM) losslessly, embed it as part of payload.

f) By means of LSB replacement, embed the value of ∂, size of LM and size of the message bits.

g) Apply inverse I-IWT and combine all the sub-bands to form the marked image.

Step 2 to 6 is performed for all the sub- bands to embed the data.

Extraction Procedure:

a) The marked image as input undergoes I-IWT and the four sub-bands LL, LH, HH, and HL are obtained.

b) By means of LSB extraction obtain the value of ∂, size of LM and the size of the message data.

c) Obtain the adjacent pixel difference sequence (d1, d2 …dM) of each sub-band.

d) Using inverse mapping of PPDE method extract the embedded bits from each embeddable pair of pixel difference value.

e) After extracting the secret message, apply inverse I-IWT to all the sub-bands and combine them to form the original image.

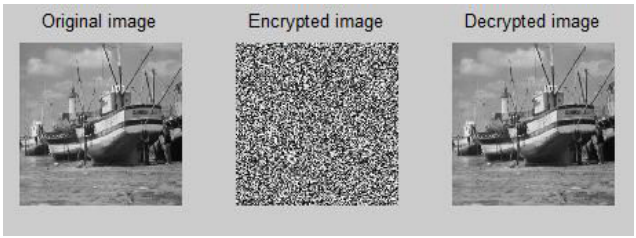
f) Step 2 to 4 needs to be performed for all sub-bands to extract the secret message.

Aim is to expand or to shift the bins in such a way that the distortion is minimum. In conventional PEE for the pair $(0,0)$ is embedded with 2 bits$(0,0), (0,1), (1,0)$ or $(1,1)$ having a distortion of 0,1,1,2 respectively. Mapping $(0,0)$ to $(1,1)$ will cause a distortion of 2. In order to reduce this distortion, mapping of $(0,0)$ to $(1,1)$ should be avoided. In new mapping each pair in $\{(0,-1),(-1,0),(-1,-1),(0,0)\}$ is embedded with log23 bits instead of 2 bits. The above mentioned four pairs are mapped to$(1,-2)$, $(-2,1)$, $(-2,-2)$ and $(1,1)$ respectively with 1 bit being embedded in each pair instead of being shifted in conventional PEE.

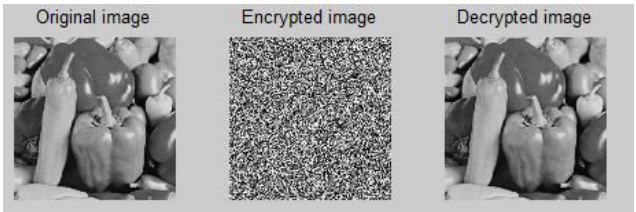
5. EXPERIMENTAL ANALYSIS AND RESULTS

In order to evaluate a successive factor associated with proposed image encryption scheme, it is necessary to calculate the outcome of image imperceptibility. The outcome of decrypted image can be only called as imperceptible if it bears nearly similar or closer value of

signal quality with the original image, so that it is hard to differentiate the signal quality of decrypted image. Moreover, the best mechanism to prove that proposed encryption method offers good security without hindering the signal quality is to judge the value of Peak Signal-to-Noise Ratio (PSNR). Some sample visual results of the proposed system are mentioned below: Figures 4 (a–c) and (d–f) shows the visual outcomes of gray scale as well as color scale image as an input. We find that there is no significant difference in the outcomes for any forms and types of images in input and hence the proposed system can be used widely for encrypting any type of images. For an effective analysis, we perform comparative analysis of nearly similar work being carried out by Singh and Singh [8]. According to the existing system approach of Singh [8], the pixels are grouped followed by calculation of public key using elliptical curve cryptosystem. Point addition is performed with the help of public key followed by de-grouping of the encrypted values and finally all the values are rearranged in order to obtain encrypted image. Although, this technique is safeguarded by image tampering attacks but certainly it is not resistive against the statistical attack that has the probability of breaking the encryption. Hence, we implement the work of Singh [8] and then improved it by applying nucleotide sequencing process where a matrix of values (0–255) is constructed on the basis of the DNA sequences. It is first scrambled by using public key followed up by construction of 3 matrixes (Step-5, 6, 7 of second algorithm) and finally followed by bitwise XORing. In order to assess this improvement, we analyze the pixel correlation in three different directions of matrix i.e. horizontal, vertical, and diagonal. Figure-5 highlights the correlation analysis for proposed system in all three matrix direction. The inference of the correlation map shown in Figure-5 proves that proposed system offers better encryption scheme in correlational value of any of the direction. We verified this outcome considering the colored image too.



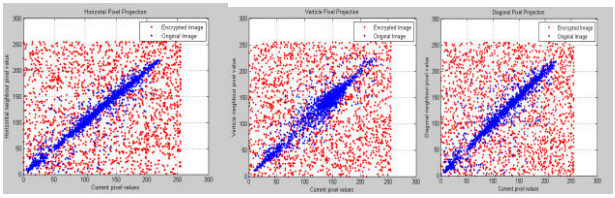
(a) Original Image (b) Encrypted Image (c) Decrypted Image



(d) Original Image (e) Encrypted Image (f) Decrypted Image

Figure-4. Visual outcomes of encryption.

For further effective analysis, we also perform comparative analysis of proposed system with respect to PSNR, Number of Changing Pixel Rate (NPCR), and Unified Average Changing Intensity (UACI) as shown in Figure-6(a), (b), (c) respectively. The complete algorithm processing time of proposed system is found to be 0.7864s on i3 processor while existing approach consumes approximately 3.5422 min on same system configuration. This outcome exhibits that proposed system offers better image encryption.



Horizontal Projection Vertical Projection Diagonal Projection

Figure-5. Analysis of correlation.

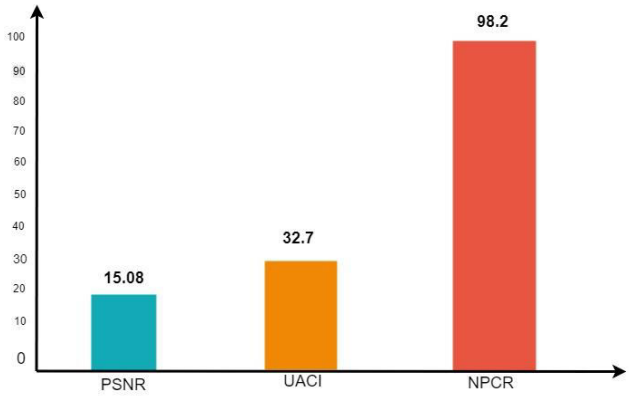


Figure-6. (a) (b) (c).

The performance analysis ECC with RDH algorithm in the proposed method is measured in terms of PSNR (dB), capacity in bits per pixel (bpp). Equations governing all the above three measures are given below:

$$\text{PSNR} = 10\log_{10}(255^2/\text{MSE})\ \text{dB} \quad (1)$$

Where MSE is the mean square error and is calculated between the cover image C and marked image C' of size $a \times b$.

$$\text{MSE} = \frac{1}{a \times b} X \sum_{i=1}^{a} \sum_{j=1}^{b} (C(i,j) - C'(i,j))^2 \quad (2)$$

The graphs shown in fig 6 depicts the histogram bins obtained for all the test images after finding the pixel difference values. Our results are compared with six other schemes listed in Table-1. The outer histogram bin curves (blue color) in Figure-6 is for Zhao et al scheme [9] and the inner curves (red color) is for the proposed scheme. Both the schemes are based on pixel differencing but Zhao's scheme is done on spatial domain while the

proposed scheme is performed in frequency domain. Even though both the schemes make room for embedding on the basis of pixel differencing, the embedding strategy is different in Zhao's scheme [9] and the proposed scheme. In Zhao's scheme embedding of bit is done based on pixel difference expansion strategy while in the proposed method it is done by pairwise pixel difference expansion.

6. CONCLUSIONS

Carrying out image encryption is not only about implementing cryptographic algorithm to cipher the image but ultimate care should be undertaken to ensure that (i) the decrypted image should maintain maximum information and signal quality, (ii) The system should offers a high quality stego image than the existing schemes at low capacity embedding (iii) key should be transferred safely with proper hiding (iv) faster process of encryption, (v) lower computational resource dependencies, (vi) ensure both forward and backward secrecy. Therefore, the proposed system implements on such technique that bears all the above mentioned characteristics The proposed study introduces novelty from all the existing approaches by incorporating an extremely lightweight encryption technique that not only maintains good pixel integrity but also offers an improved and efficient RDH method based on pairwise pixel difference expansion using integer-integer wavelet transform for securing the key. The pairwise difference expansion embedding is a novel reversible mapping that makes use of the correlations among adjacent pixel difference values. As the proposed system exhibits faster computational time hence it can be utilized for encrypting large number of images as well as it is also applicable for efficiently and effectively in hiding keys before Transmission. Elliptic curve based crypto systems can be effectively used on low resources and power system solutions such as smart cards, mobile devices, sensors and so on.

REFERENCES

Shima Ramesh Maniyath, Thanikaiselvan V., Robust & Lightweight Image Encryption Approach using Public Key Cryptosystem, Springer International Publishing AG, CSOC 2018, AISC 765, pp. 63-73, 2019.https://doi.org/10.1007/978-3-319-91192-2_7

Chen Y. C., Shiu C. W., Horng G. 2014. Encry pted signal-based reversible data hiding with public key cryptosystem. J. Vis. Commun. Image Represent. 25, 1164-1170.

Paillier P. 1999. Public-key cryptosystems based on composite degree residuosity classes. Adv. Cryptol. 1592, 223-238.

Zhang X., Long J., Wang Z., Cheng H. 2016. Lossless and reversible data hiding in encrypted images with public-key cryptography. IEEE Trans. Circuits Syst. Video Technol. 26, 1622-1631.

Miss. Nuzhat Ansaria, Prof. Rahila Shaikhb, A Keyless Approach for RDH in Encrypted Images using Visual Cryptography,science direct, Procedia Computer Science 78 (2016) 125 – 131, doi: 10.1016/j.procs.2016.02.021

Aswathy Achuthshankar, Aswin Achuthshankar2 Arjun K P3 Sreenarayanan N M, Encryption of Reversible Data Hiding For Better Visibility and High Security, science direct, Procedia Technology 25 (2016) 216 – 223

Li T., Yang M., Wu J., Jing X. 2017. Research article A novel image encryption algorithm based on a fractional-order hyper chaotic system and DNA computing. Hindawi Complex.2017, 13.

Singh L. D., Singh K.M. 2015. Image encryption using elliptic curve cryptography. In: Elsevier-Eleventh International Multi-Conference on Information Processing. 54: 472-48.

Z. Zhao, H. Luo, Z. M. Lu and J. S. Pan. 2011. Reversible data hiding based on multilevel histogram modification and sequential recovery. International Journal of Electronics and Communications (AEÜ). 65(10): 814-826.

L. Luo, Z. Chen, M. Chen, Q. Zeng and Z. Xiong. 2010. Reversible image watermarking using interpolation technique. IEEE Transactions on Information Forensics and Security. 5(1): 187-193.

K. S. Kim, M. J. Lee, H. Y. Lee, and H. K. Lee. 2009. Reversible data hiding exploiting spatial correlation between sub-sampled images. Journal of Pattern Recognition. 42(1): 3083-3096.

P. Y. Tsai, Y. C. Hu and H. L. Yeh. 2009. Reversible Image Hiding Scheme Using Predictive Coding and Histogram Shifting. Signal Processing. 89(6): 1129-1143.

Y. Hu, H. K. Lee, and J. Li. 2009. DE-Based Reversible Data Hiding With Improved Overflow Location Map. IEEE Transactions on Circuits Systems for Video Technology. 19(2): 250-260.

Fan H., Li M. 2017. Research article cryptanalysis and improvement of chaos-based image encryption scheme with circular inter-intra-pixels bit-level permutation. Hindawi Math. Probl. Eng. 2017, 11.

Z. Ni, Y-Q. Shi, N. Ansari and W. Su. 2006. Reversible data hiding. IEEE Transactions on Circuits and Systems for Video Technology. 16(3): 354-361.

C. C. Lin, W. L. Tai and C. C. Chang. 2008. Multilevel reversible data hiding based on histogram modification of difference images. Journal of Pattern Recognition. 41(1): 3582-3591.

W. L. Tai, C. M. Yeh, and C. C. Chang. 2009. Reversible data hiding based on histogram modification of pixel

differences. IEEE Transactions on Circuits and Systems for Video Technology. 19(6): 906-910.

R. Nicole. Title of paper with only first word capitalized. J. Name Stand. Abbrev., in press.

J. Tian. 2003. Reversible data embedding using a difference expansion. IEEE Transactions on Circuits and Systems for Video Technology. 13(8): 890-896.

A. M. Alattar. 2004. Reversible watermark using the difference expansion of a generalized integer transform. IEEE Transactions on Image Processing. 13(8): 1147-1156.

S. Weng, Y. Zhao, J-S. Pan and R. Ni. 2007. A novel high-capacity reversible water-marking scheme. Proceedings of IEEE International Conference on Multimedia and Expo (ICME '07), 631-634.

B. Yang, M. Schmucker, X. Niu, C. Busch and S. Sun. 2004. Reversible image watermarking by histogram modification for integer DCT coefficients. Proceedings of the 6th Workshop on Multimedia Signal Processing (MMSP '04), 143–146.

D. M. Thodi and J. J. Rodríguez. 2004. Prediction-error based reversible watermarking. Proceedings of International Conference on Image Processing (ICIP '04), 3: 1549-1552.

Y. Hu, H. K. Lee and J. Li. 2009. DE-Based Reversible Data Hiding With Improved Overflow Location Map. IEEE Transactions on Circuits Systems for Video Technology. 19(2): 250-260.

K. H. Jung and K. Y. Yoo. 2009. Data hiding method using image interpolation. Journal of Computer Standard and Interfaces. 31(1): 465-470.

Chin-Feng Lee, Yu-Lin Huang. 2012. An efficient image interpolation increasing payload in reversible data hiding. Expert systems with applications. 39: 6712-6719.

K. H. Jung and K. Y. Yoo. 2015. Steganographic Method Based on Interpolation and LSB Substitution of Digital Image Interpolation. Multimed Tools Appl. 74: 2143-2155.

R. Geetha and S. Geetha. 2016. Multilevel RDH scheme using image interpolation. 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Jaipur. pp. 1952-1956.

Bo Ou, Xiaolong Li, Yao Zhao. 2013. Pairwise Prediction-Error Expansion for Efficient Reversible Data Hiding. IEEE Transactions On Image Processing. 22(12): 5010-5021.