Randomized Symmetric Crypto Spatial Fusion Steganographic System

Viswanathan Perumal

Information Technology and Engineering, VIT University, Vellore 632014, India
E-mail: viswatry2003@gmail.com

Abstract. The image fusion steganographic system embeds encrypted messages in decomposed multimedia carriers using a pseudorandom generator but it fails to evaluate the contents of the cover image. This results in the secret data being embedded in smooth regions, which leads to visible distortion that affects the imperceptibility and confidentiality. To solve this issue, as well as to improve the quality and robustness of the system, the Randomized Symmetric Crypto Spatial Fusion Steganography System is proposed in this study. It comprises three-subsystem bitwise encryption, spatial fusion, and bitwise embedding. First, bitwise encryption encrypts the message using bitwise operation to improve the confidentiality. Then, spatial fusion decomposes and evaluates the region of embedding on the basis of sharp intensity and capacity. This restricts the visibility of distortion and provides a high embedding capacity. Finally, the bitwise embedding system embeds the encrypted message through differencing the pixels in the region by 1, checking even or odd options and not equal to zero constraints. This reduces the modification rate to avoid distortion. The proposed heuristic algorithm is implemented in the blue channel, to which the human visual system is less sensitive. It was tested using standard IST natural images with steganalysis algorithms and resulted in better quality, imperceptibility, embedding capacity and invulnerability to various attacks compared to other steganographic systems.

Keywords: *composition; decomposition; decryption; extraction; encryption; hiding; spatial fusion.*

1 Introduction

Steganographic systems embed secret data in digital cover media to make confidential information secure, whereas steganalysis breaks the steganographic system for exposing the secure data to unauthorized persons. Image steganographic systems are classified into frequency (transform) and spatial domain systems. Transform-based steganographic methods use discrete Fourier transform, discrete cosine transform or discrete wavelet transform to validate the frequency of the host signal for embedding the secret data. Fourier transform determines the magnitude of its coefficients, whereas cosine transform evaluates low-, mid-, high-frequency components to hide the secret

Received August 9th, 2014, 1st Revision October 3rd, 2014, 2nd Revision July 10th, 2015, 3rd Revision August 21st, 2015, Accepted for publication February 19th, 2016.
 ISSN: 2337-5787, DOI: 10.5614/itbj.ict.res.appl.2016.10.1.2

data. Wavelet transform hides them by decomposing the source into high- and low-frequency components. These transform domain-based methods are robust against attacks [1] but do not maintain the quality of the steg image very well. To improve robustness along with quality, region-based fusion embedding schemes are used, for example gradient pyramid [2], ratio pyramid [3], wavelet [4], and spatial fusion [5-7]. These methods evaluate prediction errors in the region of approximation in the cover image and embed the secret data by modifying the least significant bit (LSB) to a coefficient not equal to zero.

Spatial domain-based steganographic methods are LSB Matching (LSBM) [8], and LSB Replacement (LSBR) [9]. LSBR embeds by replacing the LSB, whereas LSBM and LSB Matching Revisited (LSBMR) [10] embed by matching the LSB. This technique transforms the LSB of the source into an alternate bit of secret data by increasing or decreasing randomly by 1. There are other techniques, which flip the last and second LSB of the cover image [11] governed by a score-of-distortion function [12]. These spatial domain methods are more attractive because of their high payload, but due to the critical need of robustness researchers are encouraged to focus on transform domain techniques.

Steganalysis techniques such as simple pairing and structure analysis [14-15], chisquare analyses [13], regular/singular (RS) group analyses can be used to validate the robustness of a steganographic system. Chisquare analysis evaluates the color components red, green, and blue (RGB) of the steg image to analyze the secret message. RS analysis exposes structural asymmetry artifacts in the steg image. Laplacian detector identifies the center of pixels located at sharp edges to project the difference with pixel neighbors [16]. This reduces the occurrence of higher-frequency components for matching means acting like a low-pass filter [17]. The center of mass calculated with the histogram characteristic function [18-19] reveals secret data based on this analysis but is not reliable for gray level images.

The latest steganographic techniques, such as highly undetectable steg [12], adaptive steganography [20], universal wavelet relative distortion [21], maximum mean discrepancy [22] and edge adaptive image steganography [23], are based on the principle of preserving the source model. They estimate edge pixels by evaluating the difference between adjacent pixels greater than the threshold to embed. A major drawback is missing prominent edge results when embedding in smooth regions.

In order to improve the robustness and quality, the proposed Randomized Symmetric Crypto Spatial Fusion Steganographic System includes:

1. Symmetric cryptosystem

2. Spatial fusion
3. Region-based embedding and extraction

This paper is structured as follows: Section 2 focuses in detail on the process of the proposed Randomized Symmetric Crypto Spatial Fusion Steganographic System. Section 3 describes the experimental testing and analysis of the Randomized Symmetric Crypto Spatial Fusion Steganographic System. Finally, Section 4 contains the conclusion and future work.

2 Proposed Randomized Symmetric Crypto Spatial Fusion Steganographic System

The proposed Randomized Symmetric Crypto Spatial Fusion Steganographic System consists of four stages, as illustrated in Figure 1. Each stage of the proposed system is expressed on the basis of security, quality and payload. In the first stage, secret message S is encrypted to cipher C using a four-bit key by the bitwise symmetric key symmetric crypto system, which improves the confidentiality of the secret message. In the second stage, spatial fusion is applied to the cover image I by decomposition limit D_L to decompose $I \rightarrow I_D$. It evaluates embedding region I_D^M based on sharp intensity and capacity for avoiding distortion in smooth regions and to provide high payload. In the third stage, C is embedded with key K by differencing each pixel by 1 when the intensity level is not equal to 0 and with even or odd pixel evaluation. This provides a lower modification rate to avoid distortion. Then, the decomposed regions are combined with embedded region I_C^K to provide a high level of security for the secret message. Finally, in the fourth stage, extraction of embedded region I_C^D and decryption of C with a key, improving the confidentiality of the secret message. The proposed system combines a bitwise system for encryption and embedding, which requires less computation and execution time complexity, with a region-based embedding system based on spatial fusion without loss of data, which provides robustness in the steganographic system. The system is explained in detail in the following sections.

2.1 Encryption of Secret Data

In this module, the bitwise private symmetric key crypto system encrypts the secret message S into cipher C. Symmetric key encryption, shown in Algorithm (1), first transforms the S value to a binary digit $b(i)$ of 8 digits by repeating the steps (1-3) in step 4. Then, the digits are reversed $Rev()$ in step 5. The reversed value is divided by a four-digit binary key greater than 1000. The quotient $Q()$ with 5 digits is initialized in step 6 and the remainder $R()$ with 3 digits in step 7.

The quotient and remainder are concatenated *(+)* in step 8 to get the cipher. Repeat the steps until *S* is encrypted to cipher *C*.

Algorithm 1. Symmetric Key Encryption

Step 1: A = A&&128
Step 2: S = S<<1
Step 3: b(i) = A/128
Step 4: Repeat step 1 to 3 until the decimal value is converted to an 8-digit binary value
Step 5: Reverse the 8-digit binary value: Rev(b)
Step 6: Q() = Rev(b)/K if not 5 digits add 0 to the left side
Step 7: R() = Rev(b)%K if not 3 digits add 0 to the left side
Step 8: C(i) = Q()+R()
Step 9: The 8-bit value is converted to the appropriate decimal values
Step 10: Repeat the steps until all values are encrypted

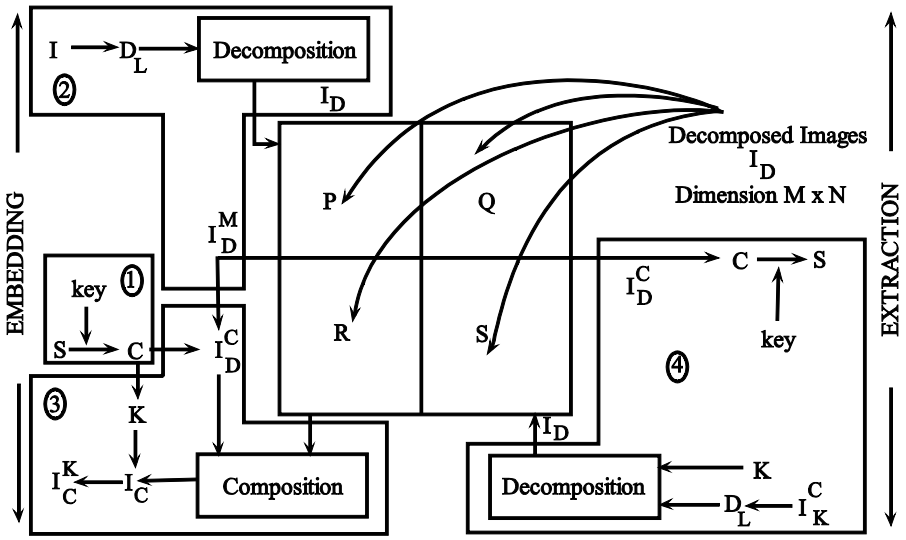


Figure 1 Symmetric crypto spatial fusion steganographic system.

2.2 Spatial Fusion Region Embedding System

The spatial fusion-based region embedding system consists of spatial fusion and a bitwise embedding system.

1. Spatial fusion decomposes the cover image into regions based on the intensity level and chooses a region with sharp intensity and high payload for embedding.

2. The bitwise embedding system embeds the secret message based on the constraints of even or odd option and not equal to zero between the region of embedding and the secret message.

2.2.1 Spatial Fusion Decomposition

Spatial fusion decomposes cover image I into four regions I_D based on the distribution of pixels. The image I with size $M \times N$ is represented as one-dimensional row vector sorted in ascending order such that $I \rightarrow I_R$. Depending on the number of limits L, intensity level D_L from I is evaluated spatially using Eq. (1). Then, D_L is used to decompose I into four regions I_D using Eq. (2).

$$\sum_{i=0}^{n} D_{\mathrm{L}}(i) = \sum_{i=0}^{R} I_{\mathrm{R}}\left(\frac{R}{i} - 1\right) \tag{1}$$

$$I_D = \underset{L=0}{\overset{3}{\forall}} \begin{cases} I < D_L \\ 0 \end{cases} \quad \text{where } D_{[0\text{-}3]} \rightarrow [P\ Q\ R\ S] \tag{2}$$

The spatial fusion method satisfies the properties of the fusion such as evaluation of the individual limit for two or more variables dependent on each variable with the expectation E such that $E\{D_1(x), D_2(y)\} = E\{D_1(x)\}, E\{D_2(y)\}$. The variable function is equal to the limit estimator function, which is continuous at that point. On the basis of asymptotic property limit estimator $D_L \rightarrow infinity$, $D_L \in I$ satisfies the constraints of probable limits, consistency and central limit theorem. Hence, it's proved that the method provides effective decomposition of I into regions I_D without loss of quality.

2.2.2 Dual Embedding and Composition with Key Initialization

Embedding is the process of hiding encrypted secret data C in a different or the same medium. The proposed approach is a dual bitwise embedding scheme, which hides C in randomly located coordinates evaluated using Eq. (3) in the decomposed regions and the key in steg image I_C. The spatial fusion selects embedding region I_D^M from I_D based on sharp intensity and having a higher number of pixels compared to other regions $I_D^M \rightarrow max\ (I_D)$. This is used to provide maximum payload and to avoid embedding distortion in smooth regions. Cipher C is embedded in the region I_D^M such that $I_D^M \rightarrow I_D^C$ by differencing each pixel by 1 with not equal to 0 constraint and even or odd pixel evaluation between I_D^M and C using Eq. (4). This approach provides a lower modification rate, which reduces distortion in I_D^M. Then the decomposed regions I_D with embedded region I_D^C are composed into steg image (I_C) using Eq. (5).

$$(x, y) = rand(1,1) \times I_D^M(i, j) \tag{3}$$

$$I_D^C(x, y) = I_D^M(x, y) - 1 \Leftrightarrow \begin{cases} \left(I_D^M \neq 0\right) \&\& \left(I_D^M \%2 \neq 0\right) \&\& \left(C = 0\right) \\ \left(I_D^M \neq 0\right) \&\& \left(I_D^M \%2 = 0\right) \&\& \left(C \neq 0\right) \end{cases} \tag{4}$$

$$I_c = I_D + I_D^C > 1 \tag{5}$$

The key (K) is evaluated in terms of type and size of C. It is embedded in the last 24 columns of the composed steg image I_C using Eq. (6) such that $I_C \rightarrow I_C^K$ and m denote the size of x and y of the steg image. K is defined as follows:

1. text data: mode 01 and count of characters
2. image: mode 02 and resolution of image

$$I_C^K(x, y) = \overset{24}{\underset{i=1}{\forall}} I_C\left(x_m, y_{m-i}\right) - 1 \Leftrightarrow \begin{cases} \left(I_C\left(x_m, y_{m-i}\right) \%2 \neq 0\right) \&\& \left(K = 0\right) \\ \left(I_C\left(x_m, y_{m-i}\right) \%2 = 0\right) \&\& \left(K \neq 0\right) \end{cases} \tag{6}$$

The proposed steganographic scheme hiding C with K through spatial fusion makes it difficult for steganalysis to locate the embedding unit, which improves the security of C. The system supports hiding of all types of secret data without any constraints and is applied in sharp intensity pixels so as to maintain the visual quality of I_C^K.

2.3 Extraction and Key Validation of Encrypted Secret Message

Extraction is the process of viewing the hidden C from ICK. The proposed extraction scheme initially extracts K by using Eq. (7), which is validated during extraction of C. Then I_C^K is decomposed by spatial fusion in the reverse process of embedding such that $I_C^K \rightarrow I_D^C$. Finally, C is extracted from decomposed region I_D^C with validation of K using Eq. (8).

$$K = \overset{24}{\underset{i=1}{\forall}} \begin{cases} 0, \left(I_C^K\left(x_m, y_{m-i}\right) > 1\right) \&\& \left(I_C^K\left(x_m, y_{m-i}\right) \%2 = 0\right) \\ 1, \left(I_C^K\left(x_m, y_{m-i}\right) > 1\right) \&\& \left(I_C^K\left(x_m, y_{m-i}\right) \%2 \neq 0\right) \end{cases} \tag{7}$$

$$C = \begin{cases} 0, \left(I_D^C > 1\right) \&\& \left(I_D^C \%2 = 0\right) \\ 1, \left(I_D^C > 1\right) \&\& \left(I_D^C \%2 \neq 0\right) \end{cases} \tag{8}$$

2.4 Symmetric Key Decryption

The symmetric key decryption in this module that decrypts C using symmetric key K is shown in Algorithm (2). It ensures the confidentiality of S, where $Cl_{bin}()$ and $S_{bin}()$ is the binary value of C and S.

Figure 2 Decomposition of color image based on intensity level of size 625 × 391 (right side) and image extracted from the decomposed region of size 66 × 66 (left side).

Algorithm 2. Symmetric key Decryption

Step 1: *The last 5 digits of C is multiplied by K;* $Cl_{bin} = C_{bin} \times K$

Step 2: *The first 3 digits of C are added with* Cl_{bin}; $Cl_{bin} = Cl_{bin} + C_3$

Step 3: *If* Cl_{bin} *exceeds 8 digits then transform to 8-bit.*

Step 4: *Reverse the digit*

$S_{bin} = circularshift(Cl_{bin})$

S_{bin} is converted into decimal data, which derives secret message S. The extracted, decrypted result is shown in Figure 2 according to the mode specified in K. This ensures that the proposed system provides secure transfer of data with authentication and verification.

3 Experimental Evaluation

The proposed system was evaluated in terms of attacks, imperceptibility, and payload with the help of a data set provided by IST [24]. It was carried out with a cover image of size 625 × 391 and secret data consisting of text and a VIT logo of size 25 × 25, 50 × 50, 65 × 65, and 80 × 80 using an Intel® Core™ i3 processor with 2.4 GHz speed and 4GB RAM.

3.1 Payload and Image Quality Analysis

The payload was evaluated by embedding different sizes of *S* in *I*. It was analyzed that the maximum payload capacity of the proposed steganographic system allows a 75% embedding rate in bits per pixel (bpp). The image quality was analyzed by peak signal noise ratio (PSNR) and modification rate. This ensures the quality of *S* in addition to the imperceptibility of *C*. The evaluated

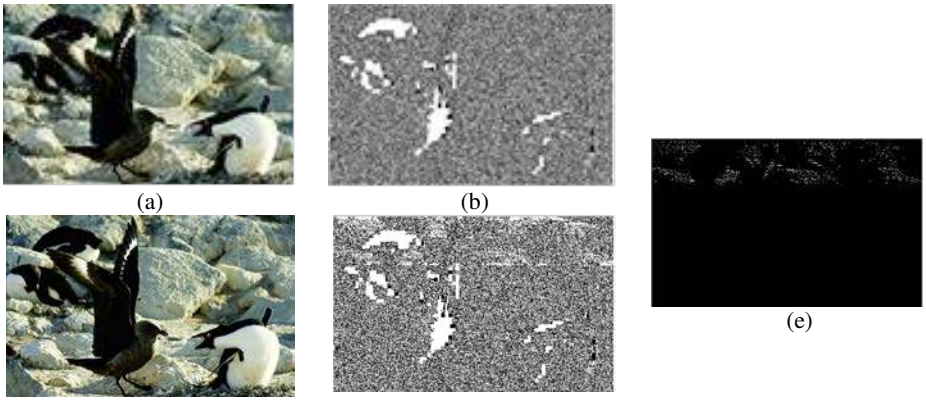


Figure 3 (a) *I*; (b) LSB of *I*; (c) 30 % embedding rate I_C^K ; and (d) LSB of I_C^K in (c);(e) LSB *I* (b) - LSB I_C^K (d).

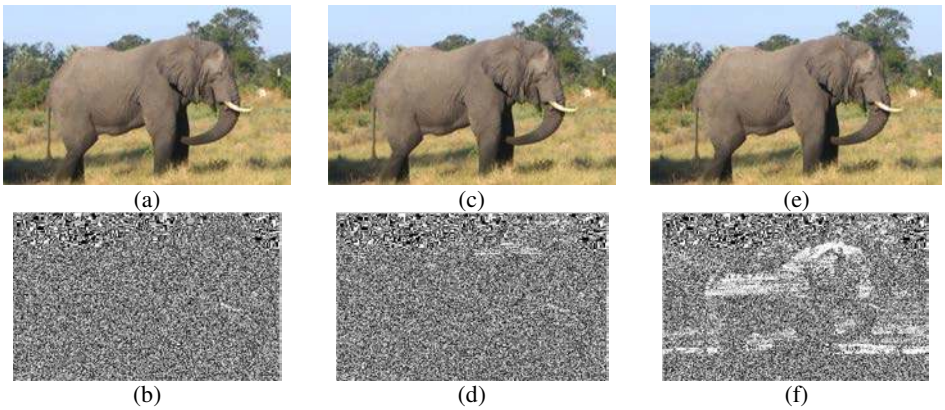


Figure 4 (a) *I*; (b) LSB (*I*); (c) 30% embedding rate I_C^K; and (d) LSB 30% embedding rate I_C^K; (e) 75% embedding rate I_C^K; and (f) LSB 75% embedding rate I_C^K.

average PSNR for the proposed Selected Least Significant Bit (SLSB) based on spatial fusion was lower compared to the LSBMR due to the readjustment of the embedding unit. The image modification rate was evaluated by taking the

difference between pixels of I_C^K and I from the same origin. Figure 3 shows only a small modification rate, especially in Figure 3(e). Extensive experimenting showed that there were no additional visual artifacts in the steg image with embedding rates from 10% to 75%, as illustrated in Figures 4 and 5. This reflects that only less smooth regions are affected by embedding S in sharp intensity in edge regions chosen by the spatial fusion, unidentifiable by the human visual system.

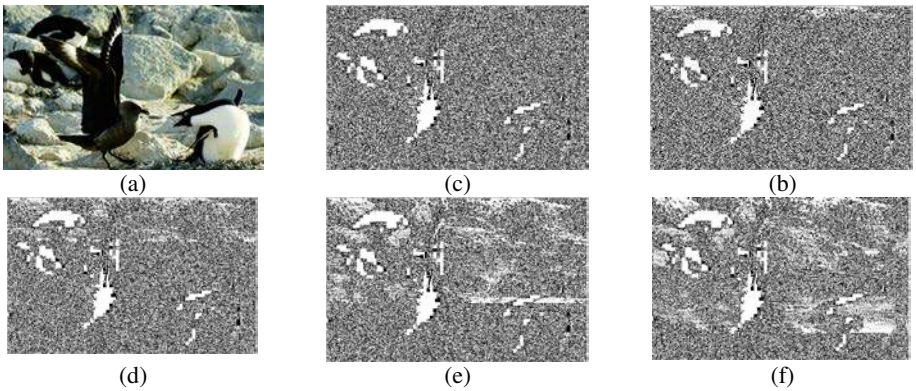
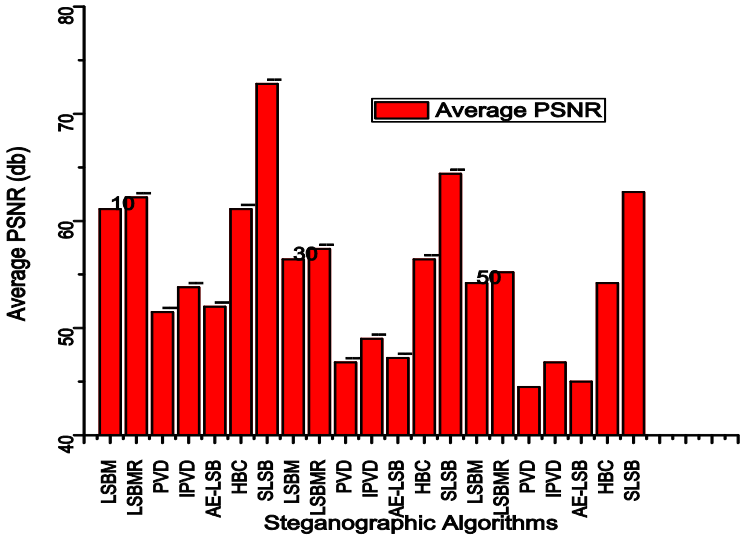
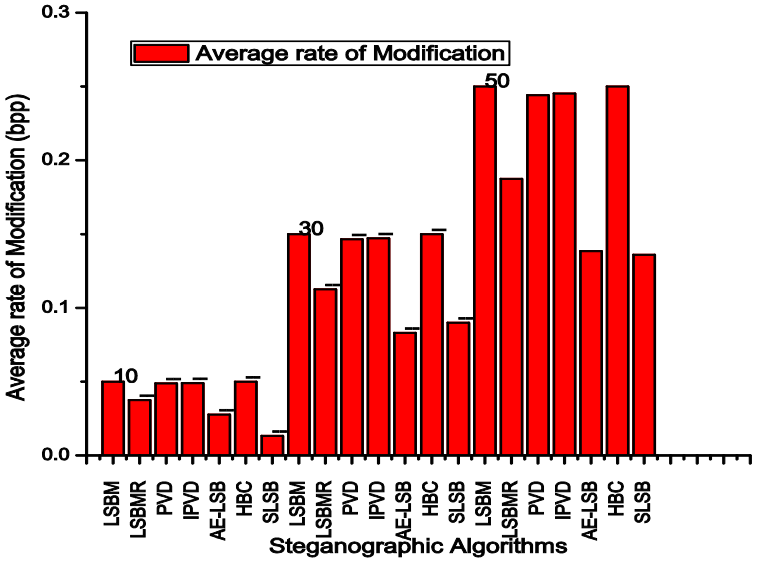


Figure 5 (a) *I*. (b) I_C^K at embedding rates of 10%, (c) 20%, (d) 30%, (e) 50%, and (f) 75%.



(a)



(b)

Figure 6 (a) Average PSNR evaluation of 1000 ICK at embedding rates of 10%, 30%, and 50%, compared to other LSB and edge-based methods. (b) Average modification rate of ICK at embedding rates of 10%, 30%, and 50%, compared to other LSB and edge-based methods.

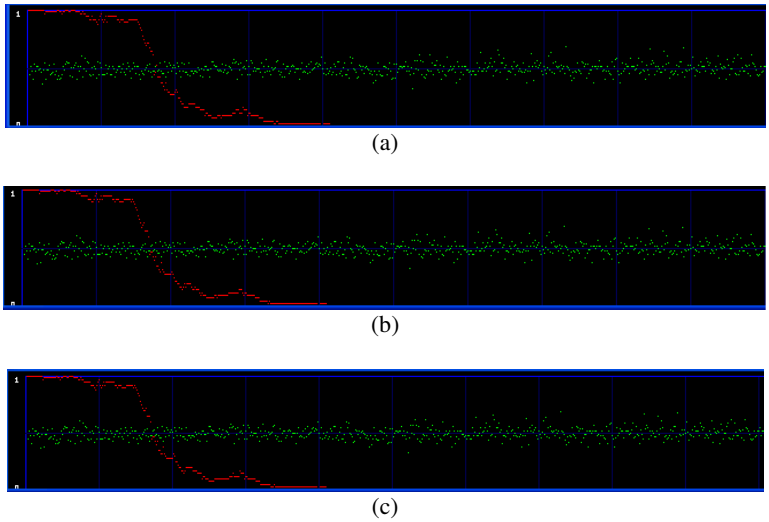
The proposed approach was matched with other LSB approaches for image quality analysis using PSNR and modification rate. Figure 6 illustrates high subjective quality compared with seven existing steganographic methods. The LSBM and hiding behind corners was equal to a 3/2 or 4/3 modification rate of LSBMR. The LSBMR, LSBM and pixel value differencing methods based on a random embedding scheme inevitably disturb the smooth regions at higher modification rates. The SLSB method disturbs the sharp regions with a lower modification rate, thus maintaining the quality of the steg image.

3.2 Statistical Attack

A statistical attack analysis of the proposed system was conducted using the chi-square test [25], as shown in Figure 7. Analysis of the different curves shown in a grid of blue curves having the representation 1 indicates hidden data. The red curve determines the probability pairs of values (PoVs) with random distribution derived from start to successively larger amounts of pixels in the image. If they are equal to 1, the PoVs are random, which means there is a message hidden in the LSBs. If they are equal to 0, then the random distribution results in a false positive, but this is supposed to be less frequent. If they are equal to 0, then not random means there is no hidden message in the LSBs. The

average value of all LSBs in each block of pixels, being 128 by default, is displayed in green.

The proposed system was applied in the Invisible Secrets 2002 steganalysis software, which is used to identify hidden messages. It reported that "the file does not seem to contain hidden data" for all I_C^K, which shows that statistical attacks are impossible.



(a) (b) (c)

Figure 7 (a) Chisquare analysis of ICK at embedding rates of 30%, (b) 50%, and (c) 75%.

3.3 Complexity Analysis

The time complexity and computational complexity of the proposed algorithm was evaluated through estimating the execution time of encryption with embedding and of extraction with decryption. Table 1 illustrates the minimal

Table 1 Quality and execution time analysis.

I **(LENA) Size**	***C*** **(Logo)**	**PSNR**	**Modification Rate**	**Hiding time with encryption (secs)**	**Extraction time with decryption (secs)**
512 × 512	25 × 25	73.2085	0.00003	11.2129	7.230889
512 × 512	45 × 45	68.1484	0.001	12.55523	8.930648
512 × 512	60 × 60	64.774	0.0023	14.20284	9.229091
512 × 512	80 × 80	63.1043	0.0033	16.25818	9.253179
256 × 256	25 × 25	67.0816	0.0013	11.21576	6.453152
256 × 256	45 × 45	61.9812	0.0042	11.87344	6.749656

time of execution and good quality analysis in terms of PSNR and modification rate. The PSNR of I_C^K was more than 60 db and the modification rate was a very small, trivial value, which indicates high imperceptibility of C and quality of I_C^K. The time complexity for embedding with encryption was less than 16 sec and for extraction with decryption less than 10 sec, which indicates that the proposed system has low computation and time complexity.

3.4 RS Analysis

RS analysis is used to extract data having LSB replacement and moreover estimates the amount of hidden data. It is determined by structural asymmetry artifacts between R and S.

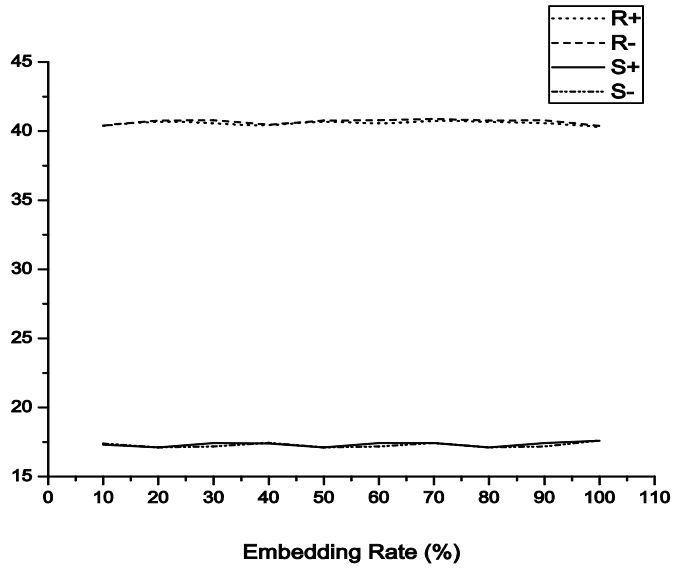


Figure 8 RS diagram of I_C^K.

4 Conclusion

The proposed Spatial Fusion Symmetric Crypto Steganographic System evaluates the content of a cover image to embed encrypted messages in a sharp edge region while preserving the statistical and visual qualities of the steg image. The symmetric key bitwise encryption of a secret message embedded in the region evaluated by spatial fusion ensures the security and confidentiality of the secret message. Experimental testing and statistical attack analysis using various steganalysis algorithms revealed a high security level and visual quality compared to other LSB edge-based approaches. The proposed system has less computation and execution time complexity for encryption, hiding and

extraction compared to other approaches. The proposed system can be extended to audio and video data if the maximal amount of cover is higher than the embedding rate.

References

[1] Harmsen, J. & Pearlman, W., *Steganalysis of Additive Noise Modelable Information Hiding*, Proc. SPIE Electronic Imaging, **50**(20), pp. 131-142, 2003.

[2] Xydeas, C.S. & Petrovic, V., *Gradient based Multiresolution Image Fusion*, IEEE Transactions on Image Processing, **13**(2), pp. 228-237, 2004.

[3] Toet, A., *Image Fusion by a Ratio of Low-pass Pyramid*, Pattern Recognition Letters, (9), pp. 245-253, 1989.

[4] Viswanathan, P. & Venkata Krishna, P., *Text Fusion Watermarking in Medical Image with Semi-reversible for Secure Transfer and Authentication*, Advances in Recent Technologies in Communication and Computing, IEEE explore, pp. 585-589, Oct. 2009.

[5] Viswanathan, P. & Venkata Krishna, P., *Fusion of Cryptographic Watermarking Medical Image System with Reversible Property*, ICTACT Int J. on Image and Video Processing, **2**(1), pp. 258-263, 2011.

[6] Viswanathan, P. & Venkata Krishna, P., *Medical Image Spatial Fusion Watermarking System*, Signal and Image Processing, Lectures Notes in Electrical Engineering, **222**, pp. 453-464, 2013.

[7] Viswanathan, P. & Venkata Krishna, P., *A Joint FED Watermarking System using Spatial Fusion for Verifying the Security Issues of Teleradiology*, Biomedical and Health Informatics, IEEE Journal of, **18**, (3), pp. 753- 764, 2014.

[8] Ker, A., *Improved Detection of LSB Steganography in Grayscale Images*, Lecture Notes in Computer Science, International Workshop on Information Hiding, eds. Fridrich, pp. 97-115, 2004.

[9] Chan, C-K. & Cheng, L-M., *Hiding Data in Images by Simple LSB Substitution*, Pattern Recognition letter, **37**(3), pp. 469-474, 2004.

[10] Ker, A.D., *Steganalysis of LSB Matching in Grayscale Images*, IEEE Signal Process. Letter **12**(6), pp. 441-444, 2005.

[11] Pevnỳ, T., Filler, T. & Bas, P. *Using High-dimensional Image Models to Perform Highly Undetectable Steganography*, Lecture Notes in Computer Science: 12th International Conference on Information Hiding, (ed.(s)). Safavi-Naini R, Böhme R, Fong PWL, pp. 161-177, 2010.

[12] Ker, A.D., *Steganalysis of Embedding in Two Least-significant Bits*, IEEE Trans. Inf. Forensics Security **2**(1), 46–54, 2007.

[13] Westfeld, A. & Pfitzmann, A., *Attack on Steganographic Systems*, Lectures Notes in Computer Science, **1768**, pp. 61-75, 2000.

[14] Fridrich, J., Goljan, M. & Du, R., *Detecting LSB Steganography in color, and gray-scale images*, *IEEE Multimedia*, **8**(4), pp. 22-28, Oct. 2001.

[15] Dumitrescu, S., Wu, X. & Wang, Z., *Detection of LSB Steganography via Sample Pair Analysis*, *IEEE Trans. Signal Process.*, **51**(7), pp. 1995-2007, 2003.

[16] Wu, D. & Tsai, W., *A Steganographic Method for Images by Pixel Value Differencing*, Pattern Recognit. Letter, **24**, pp. 1613-1626, 2003.

[17] Zhang, X. & Wang, S., *Vulnerability of Pixel-value Differencing Steganography to Histogram Analysis and Modification for Enhanced Security*, Pattern Recognit. Letter, **25**, pp. 331–339, 2004.

[18] Yang, C.H., Weng, C.Y., Wang, S.J. & Sun, H.M., *Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems*, IEEE Trans. Inf. Forensics Security, **3**(3), pp. 488-497, 2008.

[19] Hempstalk, K., *Hiding behind corners: Using Edges in Images for Better Steganography,* Proc. Computing Women's Congress, Hamilton, New Zealand, 2006.

[20] Kouider, S., Chaumont, M. & Puech, W., *Adaptive Steganography by Oracle (ASO)*, IEEE International Conference on Multimedia and Expo (ICME), pp. 1-6, July 2013

[21] Holub, V., Fridrich, J. & Denemark, T., *Universal Distortion Function for Steganography in an Arbitrary Domain*, EURASIP J. Inform. Security, **2014**(1), 2014.

[22] Filler, T. & Fridrich, J.*, Design of Adaptive Steganographic Schemes for Digital Images*, Media Watermarking, Security, and Forensics XIII, Part of IS&T SPIE Electronic Imaging Symposium, 7880, pp. 1-14, 2011

[23] Luo, W., Huang, F. & Huang, J., *Edge Adaptive Image Steganography Based on LSB Matching Revisited*, IEEE Trans. Inf. Forensics Security **5**(2), pp. 201–214, 2010.

[24] IST image data set http://wang.ist.psu.edu/docs/related/downloads (9 November 2013).

[25] Steganography attack tools http://guillermito2.net/stegano/tools/ (9 November 2013).