ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 9(39), DOI: 10.17485/ijst/2016/v9i39/86519, October 2016*

Enhanced Playfair Cipher for Image Encryption using Integer Wavelet Transform

Sudharshan Chakravarthy[1]*, S. Prasanna Venkatesan[1], J. Madhav Anand[1] and J. Jennifer Ranjani[2]

[1]School of Computing, SASTRA University, Thanjavur - 613401, Tamil Nadu, India;
chakravarthy.sudharshan@gmail.com, spvtnj@gmail.com, jmadhavanand@gmail.com
[2]SASTRA University, Thanjavur – 613401, Tamil Nadu, India;
jenny@cse.sastra.edu

Abstract

Objective: In this contemporary social networking era, it is no bewilderment that, information security breach is at its epitome, especially on texts/images. Thus there is a requisite for integrity for information to be transmitted over an insecure channel. Thus image/text encryption plays a vital preprocessing role in contemporary data transmission. **Method**: This paper analyses the performances of four novel, lossless methodologies of implementing the enhanced Playfair cipher in spatial and frequency domains, with integer wavelet transform (IWT) through lifting scheme. **Findings**: The proposed methods involve a spatial domain algorithm being applied to the frequency domain of the images for encryption which gives out better desired error metrics. **Application**: The most feasible method out of these proposed approaches can be chosen either as a stand-alone encryption and transmission mechanism or a pre-requisite step for that specific image in steganography and watermarking.

Keywords: Enhanced Playfair Cipher, Integer Wavelet Transforms, Image Encryption, Internet Security, Lifting Scheme

1. Introduction

The potential risks that many internet users face today is the loss of data integrity and privacy. Cryptography is the process of encrypting secret messages so that only the transmitter and the receiver can decipher it, using a key[1,2]. The other key techniques in image security are steganography and watermarking. Steganography involves the concealment of secret data into the cover data (image, audio, text or complicated biometric formats[3]).The main drawback here, which when used on a stand-alone basis lacks an extra layer of security which image encryption provides. Furthermore, watermarking is vividly used for legal data authentication, to prevent illegal data distribution and copyright protection[4]. Thus, integrity of the ownership information embedded into the host media is essential. This is brought about only by a light-weight and fast pre-processing step of encryption. Thus four different methodologies are proposed in the two possible domains, viz. spatial and frequency domain, and the best among which is suitable is chosen for further processing.

Any watermarking or steganography technique can be broadly classified into two domains: the spatial and transform domain. In spatial domain, least significant bit (LSB) and enhanced LSB methods have been proposed in the[5-7]. Walsh-Hadamard Transform, Discrete Cosine Transform (DCT)[8], Discrete Wavelet Transform (DWT)[8], Integer Wavelet Transform (IWT)[9] and Singular Value Decomposition (SVD)[8] are some transform domain watermarking and steganography techniques. Recently, a few combinations of the transforms specified have been found to be more effective than being used alone[8]. This

*Author for correspondence

paper emphasizes on IWT in the frequency domain by innovatively encrypting the coefficients of several bands in various levels and comparing the results with the conventional spatial domain encryption. IWT is implemented using lifting scheme, due its lossless data extraction capabilities, computational speed and in-place generation of coefficients[9,10].

Playfair cipher is a symmetric, digraph substitution cipher with a traditional 5x5 combination key-space [2,4]. In this paper, an enhanced Playfair cipher is used. Furthermore, due to less computational overhead, Playfair cipher is ideal for pre-processing mechanisms. In this paper, a 16x16 key combination is used, and has a humungous key-space of about 256! (8.578177×10^{506}). A comparative study of applying this encryption method in various scenarios in spatial and transform domain using IWT is implemented and the best method is also suggested. In the method proposed in[4] there is significant loss when the neighboring pixels are odd and equal. The proposed method resolves this issue. Thus, it is evident that using light-weight methods can be beneficial as a preprocessing step.

Section II elaborates on an introduction to IWT and Playfair cipher being used and depicts the proposed methodology, wherein the four methods are illustrated. Section III contains the results and discussions, and finally section IV discusses the conclusions.

2. Proposed Methodology

This proposed algorithm has the versatility to adapt text or an image as the plaintext to feed the designed encryption engine. The type of key used is symmetric. The overall flowchart is as shown in *Figure. 1*

Initially the pre-processed data (text (or) image) is transmitted to the generic Encryption engine (as shown in the flowchart) where, an IWT contriver, which generates the bands with respect to the variations illustrated in the subsequent sections. The key-matrix is generated for the Playfair cipher and the cipher text/image is obtained.

2.1 Pre-Processing Step

For all the pixels in the image, do the following steps,

- Retrieve the median bits (4^{th} and 5^{th} bits)
- Perform XOR operation between 2 most significant bits (MSBs) and the median bits
- Perform XOR operation between 2 LSBs and the median bits

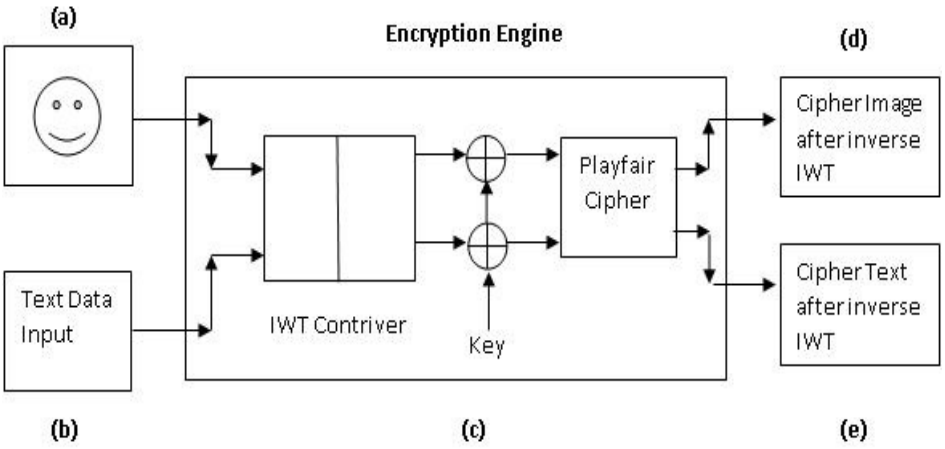

Figure 1. (a) - Preprocessed image to be encrypted, (b) – Pre-processed text data to be encrypted, (c) The Encryption engine – which consists of the IWT contriver, Key-generation module and the Playfair cipher block. (d, e) - Encrypted image and text after inverse IWT.

- Reverse the upper nibble
- Set the new pixel value to the value obtained

This pre-processing step significantly improved error-metric values, when experimentally verified.

2.2 Integer Wavelet Transform

The data transformation and its lossless reconstruction is a necessary pre-requisite for encryption engines to work. Thus, in this paper, IWT is utilized[11,12] as shown in *Figure. 2*

The proposed methods require the novel procedure of encrypting the IWT coefficients obtained from various sub-bands of the IWT. IWT provides a computationally efficient and lossless form of decomposition[13,14]. IWT is performed on an image (or a sub-level) using the lifting scheme, as described in[15] where four sub-bands are obtained, and represented by the following notations:

1. LL - Resultant of the application of low-pass filtering in vertical and horizontal directions; denotes the approximation image.
2. HL - Resultant of horizontal high-pass vertical low-pass filters; denotes the vertical details.
3. LH - Resultant of vertical high-pass and horizontal low-pass filters; denotes the horizontal details.
4. HH - Resultant of high-pass filters in both directions; denotes the diagonal details.

2.3 Encryption using Playfair Cipher

Playfair cipher is a symmetric, digraph substitution cipher with a traditional 5x5 combination key-space as described by [2].

2.3.1 Algorithmic Steps for Playfair Cipher

A 16x16 matrix is chosen as a key matrix, since a coherent range of 0-255 is used for both images (as gray values) and text (ASCII); wherein values are filled in a random manner. Since a 16x16 key combination is used, and has a surfeit key-space, when compared to the conventional Playfair cipher as shown. Thus, using a light-weight method like this can be beneficial as a preprocessing step.

Key-space ratio on comparison with traditional

$$\text{Playfair cipher} = \frac{256!}{25!} = 1.55 \times 10^{25}$$

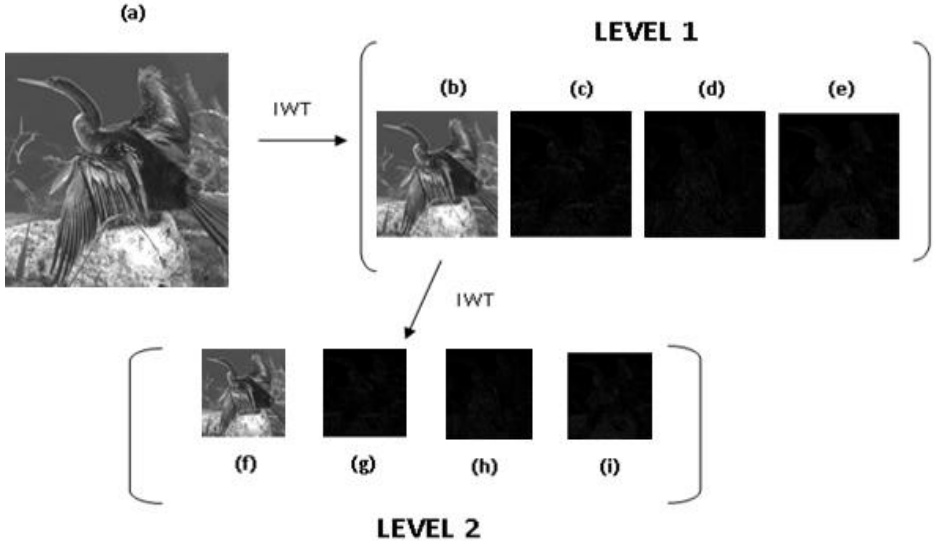

Figure 2. Resultant of two-level IWT performed on 'bird' (a) - Input image, (b) To (e) – level 1 – LL, LH, HL and HH respectively. (f) To (i) – level 2 – LL2, LH2, HL2 and HH2 respectively.

Then, for each adjacent pair of pixels,

a. Mapped integers in the same row of key-matrix are right-shifted by one position; this is done in a circular fashion for the right-most column cells.
b. If the mapped characters are in the same column, then a bottom-shift is done, with a circular replacement for the last row values.
c. When mapped characters are found in the same cell of key matrix, it is replaced by the right-diagonal element in the key-matrix. This is done to prevent data loss due to approximation, which is a main drawback in method proposed by[4].
d. For the final pair of pixels, replace the values in the opposite side of the row in the rectangle formed by the mapped values.

The encrypted histograms and contour analysis are as shown for 'lion', 'Lena' and 'boat' in *Figure. 3*

2.3.2 *Key-space, Search-space and Frequency Analysis*

Key–space is an important metric by which an encryption algorithm is valued because, larger the key-space, more difficult it is to try out the key in a trivial trial-and-error method. Search-space has also considerably improved, which increases the resistance to brute-force attack. It can be defined as the amount of di-grams (in the case of Playfair cipher) the intruder has to refer in order to figure out the relation between a given pair of pixels. This in turn facilitates in the frequency analysis of the variation of the cipher used. Lower the frequency of occurrence of cipher-values, greater is the security provided.

The key-space, search-space and frequency analysis of the method used as compared to many other Playfair implementation methods in the papers[3,4,11,12] and shown in *Table1*.

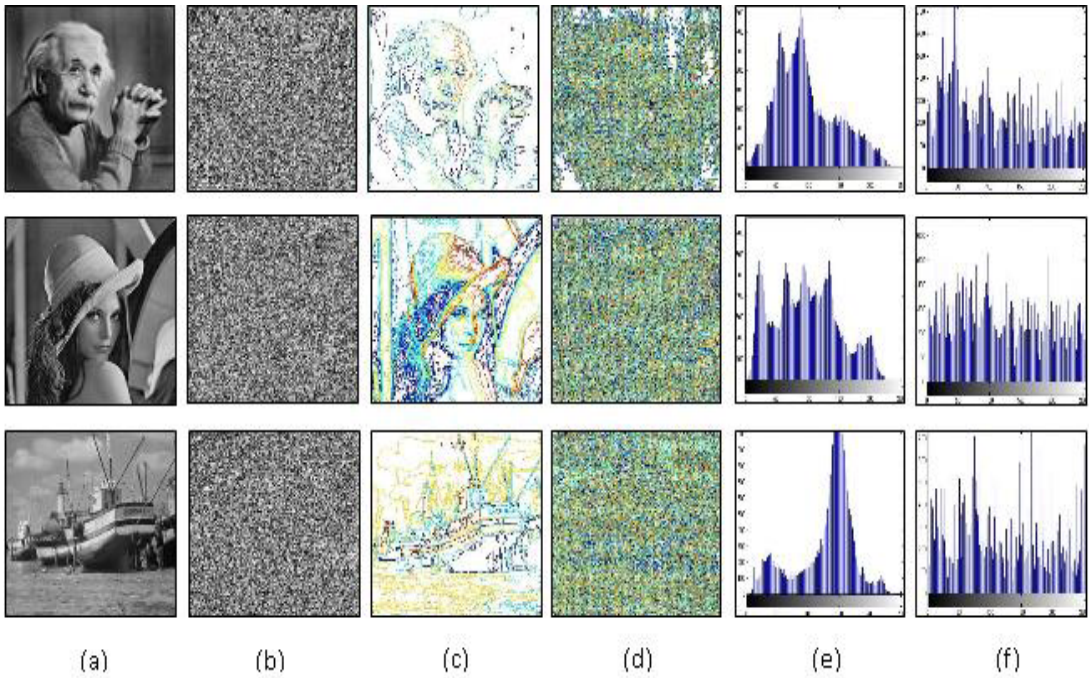

Figure 3. Playfair cipher analysis (a) - Input image-set, (b) – Playfair encrypted images in spatial domain, (c) - input's contour plot, (d) – contour plot of encrypted images, (e) – input's histogram plot, (f) – histogram plot of encrypted images.

Table 1. Key-space, search-space and frequency analysis

	Aftab's Method[11]	Nitin's Method[12]	EPC
Key-space	3.0488×10^{29}	1.2688×10^{89}	8.5781×10^{506}
Search-space	784	4096	65536
Frequency	0.0357	0.0156	0.0039

2.4 Encryption

The following sub-sections yield four novel encryption paths, which has a common framework structure as enumerated above, with the finer discrete details varied.

2.4.1 Enhanced Playfair Cipher (EPC)

This segment is the most trivial of all the methods, since this involves no transform domain. The given image/text is directly pre-processed (forward) and encrypted using the key-matrix generated. The key system used here is symmetric key system, since the same key is used for both encryption and decryption process. Performance, computation and time analysis is emphasized in the upcoming section. The following flow diagram, *Figure. 4*, elucidates the approach:

2.4.2 Single Level IWT – Encrypt LL Band (SLILL)

This component consists of two major sub-processes: application of single level IWT and Playfair cipher encryption. Obtain the input image I, and is pre-processed (forward). Apply IWT on I (1st level), to procure the decomposed components LL (approximate band, low frequency) and [LH, HH, HL] which constitute the high frequency coefficients. The in- range (0 - 255) values from LL are collected and arranged in the raster-scan order.

On the contrary to the embedding process, where the high frequency bands are used[16,17], the LL (cA) band is encrypted since it contains the most significant information. Thus, LL after encryption yields LL'. The components are reconstructed using LL', LH, HL, HH to get the

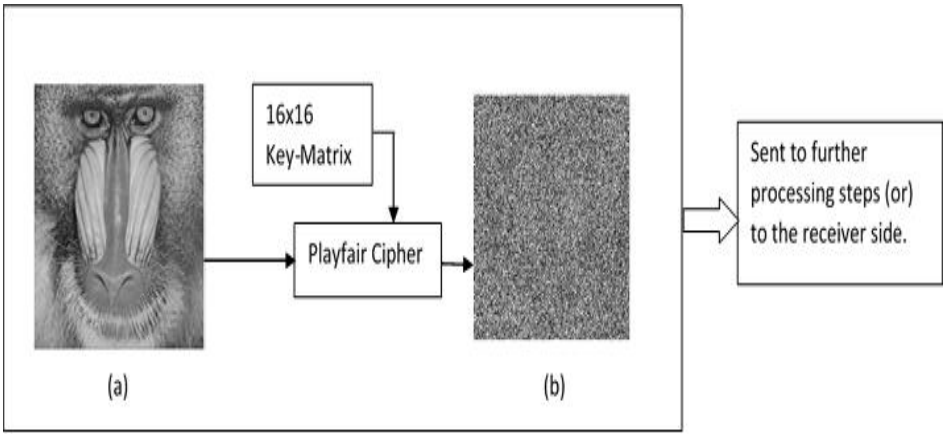

Figure 4. (a) - baboon – to encrypt , (b) – Playfair encrypted image.

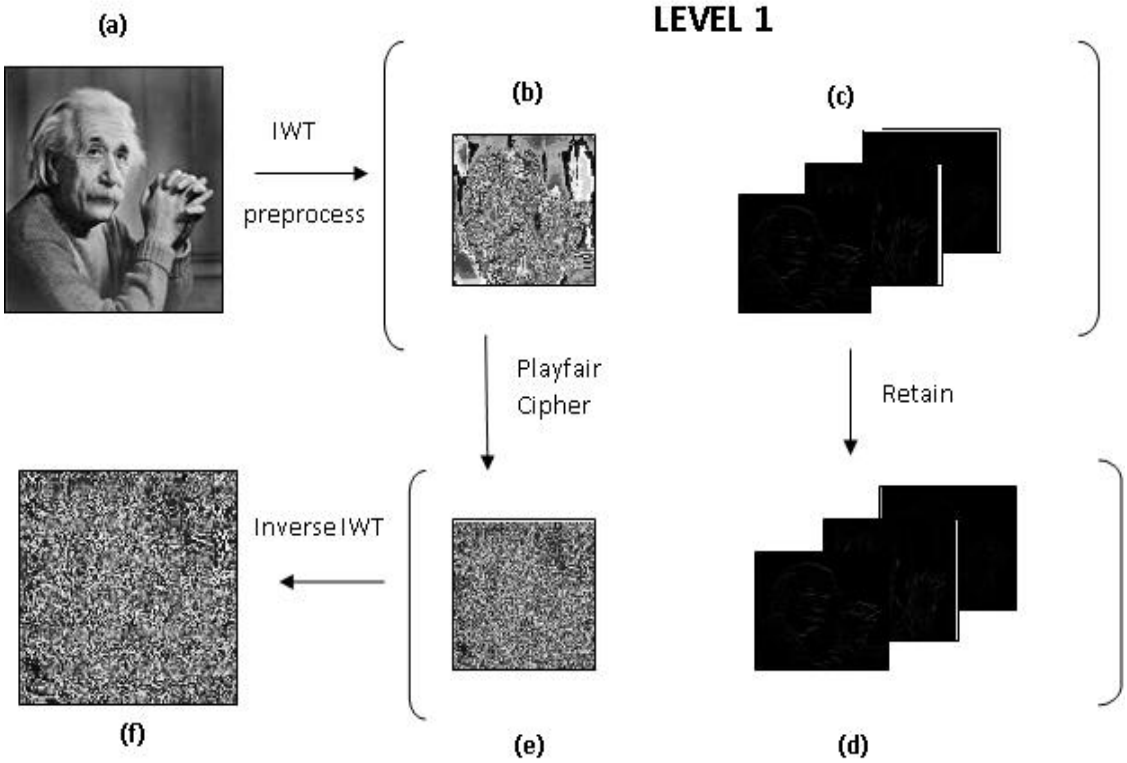

Figure 5. (a) - Image Input, (b) – LL after applying IWT, (c) – LH,HL and HH bands of IWT of 'Einstein' image, (d) – The retained bands, (e) – Encrypted LL - band, (f) – Reconstructed, encrypted 'Einstein'.

encrypted image I'. Image I' is the nested secure image, and is obtained in encrypted form.

The method is further instantiated by the following flow diagram, *Figure. 5*, which uses the 'Einstein' image:

2.4.3 Single Level IWT – Encrypt all Decomposed Bands (SLIA)

All the bands, after checking for the range, as in the previous method, are encrypted, and denoted by LL', LH', HL', HH'. The components are reconstructed using LL', LH', HL', HH' to get the encrypted image I'. Image I' is the nested secure image, and is obtained in encrypted form, as depicted in *Figure. 6*.

2.4.4 Double - Level IWT – Encrypt LL1 and LL2 Bands (DLILL)

After getting the initial input image, level 2 IWT is performed as shown in *Figure. 2* of section *2.2*, to obtain LL_2, LH_2, HL_2, HH_2. The step of acquiring only in-range **(0 - 255)** values from LL_2, and are arranged in raster-scan order. The values are then encrypted via the Playfair cipher. Then, with the retained second level high frequency bands, a LL_1' is revamped. The same activity is performed on the newly constructed LL_1' band and the reconstruction is done from the retained first level transformation. Image (h) is the nested secure image, and is obtained in encrypted form, as in *Figure. 7*.

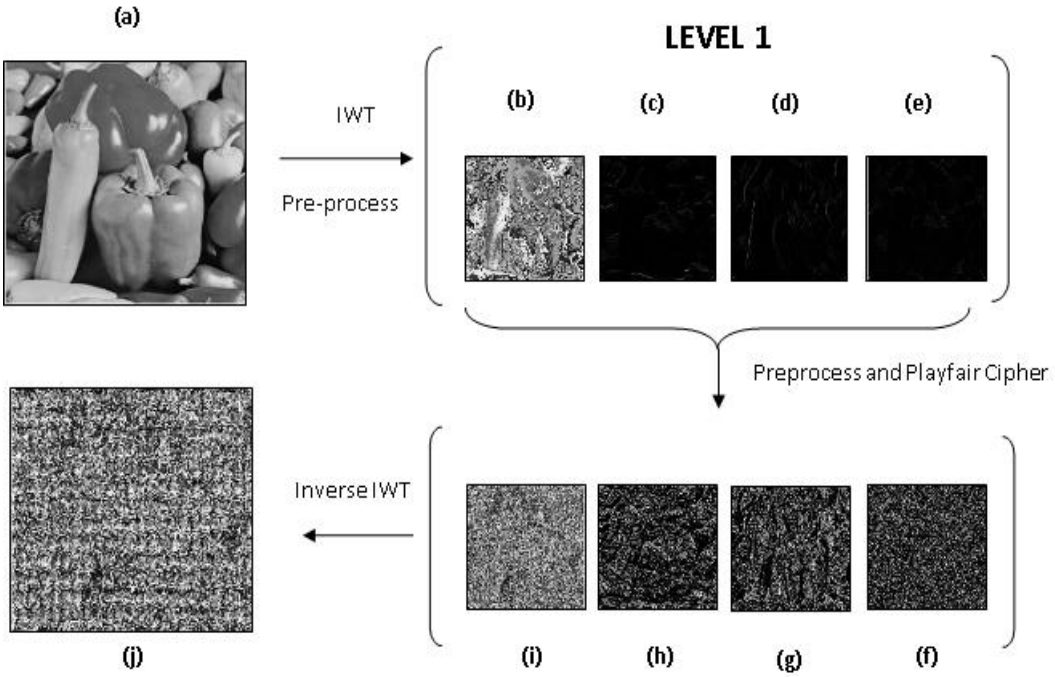

Figure 6. (a) – Covert Image 'Peppers', (b) to (e) – Decomposed set after applying IWT to 'Peppers' image, (f) to (i) – Preprocessed and encrypted counterparts of the bands, (j) – Recreated, encrypted image.

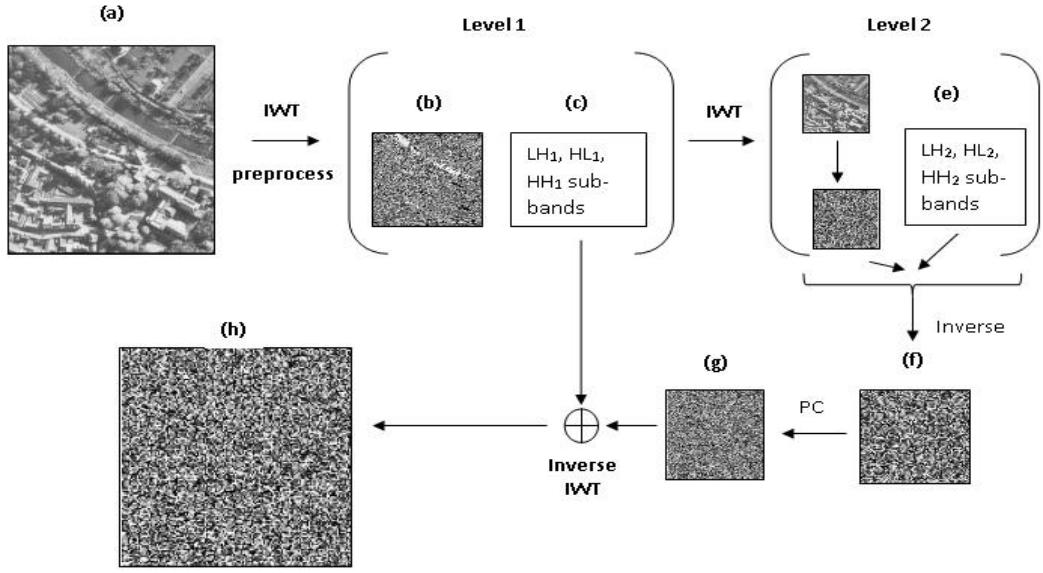

Figure 7. (a) – Secret image 'Aerial', (b) and (c) – Decomposed set of bands after applying IWT to 'Aerial' image, (d) – LL2 sub-band preprocessed and encrypted by Playfair cipher (PC in diagram) to yield LL'2 (f) – Inverse IWT performed with (e) and result of (d), (g) –Preprocessed, encrypted image, (h) Inverse IWT performed using (c) and (g).

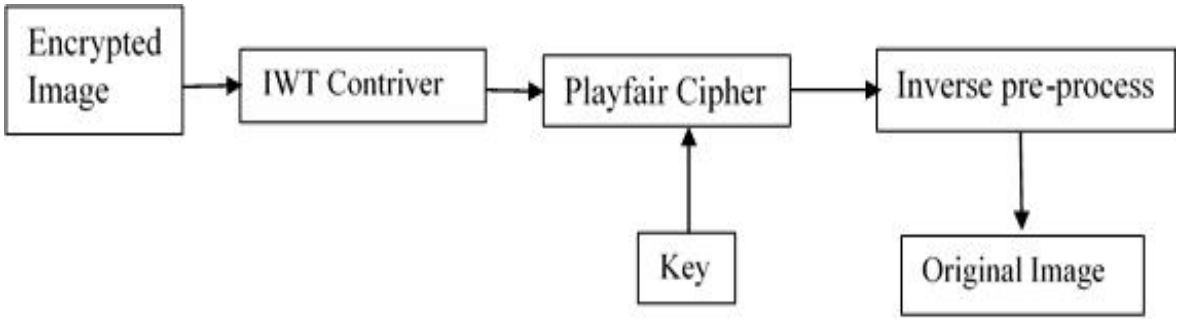

Figure 8. Decryption process at receiver's side.

2.5 Decryption

The decryption algorithms for all the above procedures are literally the exact reverse process (intuitively obtainable by minor modifications such as reversing the operations) of the encryption process.

Since we use symmetric key-encryption, same key is used for decryption and the conventional assumption of key-combination(s) distribution between the dispatcher and the receiver holds.

The general flowchart for the decryption process is shown in *Figure. 8*.

3. Experimentation Results and Analysis

3.1 Tabulation of Resultant Images

The results are delineated with the implementation of *Figure. 9*, which consists of six result-sets of 256 **x** 256 gray-scale images from the USC-SIPI Image database and simulations done with MATLAB 2013a. The images selected include 'Einstein', 'baboon', 'cameraman', 'boat' ,'bird' and 'Lena', with the procedure name represented by the sub-section at which it was introduced, in the preceding pages. The analysis of the results obtained succeeds this section.

3.2 Analysis and Error Metrics

3.2.1 d-PSNR, e-PSNR, MSE and Correlation Values

Correlation values (*Table. 2*), Structural SIMilarity (SSIM) (*Table. 3*), Peak Signal to Noise Ratio[18] (PSNR) (*Table. 4*) and Mean Square Error[18] (MSE) (*Table. 5*) are error metrics used to evaluate the effectiveness of the image encryption undertaken. d-PSNR is decrypt-PSNR, which is a measure of PSNR considering original image and the final decrypted, and e-PSNR is the PSNR value when the original and the encrypted image. The former

Table 2. Correlation co-efficient analysis

	EPC	SLILL	SLIA	DLILL
Bird	-0.0395	-0.0442	-0.0509	-0.0133
Lena	-0.0355	-0.0367	-0.0378	-0.0025
Baboon	-0.0214	-0.0252	-0.0287	0.0010
Einstein	-0.0104	-0.0063	-0.0079	-0.0032
Boat	0.0163	0.0075	0.0005	0.0131
Cameraman	-0.0321	-0.0351	-0.0377	0.0156

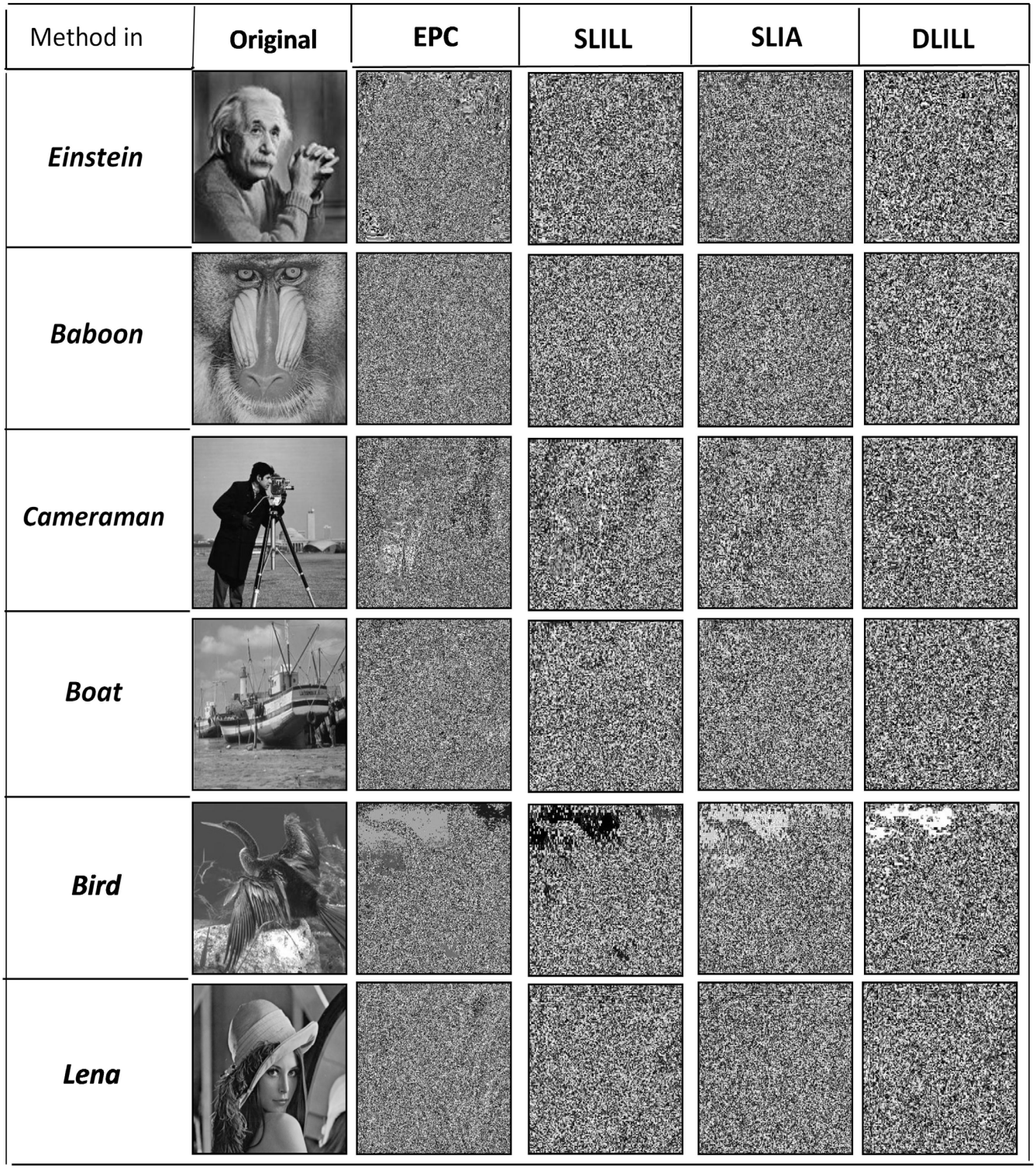

Figure 9. Tabular for visual comparison of the four proposed methods.

Table 3. SSIM analysis

	EPC	SLILL	SLIA	DLILL
Bird	0.0209	0.0119	0.0115	0.0160
Lena	0.0048	0.0046	0.0045	0.0076
Baboon	0.0025	0.0024	0.0019	0.0075
Einstein	0.0085	0.0078	0.0077	0.0078
Boat	0.0111	0.0104	0.0094	0.0103
Cameraman	0.0082	0.0081	0.0071	0.0082

Table 4. PSNR

	EPC	SLILL	SLIA	DLILL
Bird	8.1893	6.1384	4.8215	6.9493
Lena	8.4231	6.8075	5.5020	6.8429
Baboon	9.6862	6.5385	5.4797	7.2426
Einstein	8.5511	6.9967	5.2930	7.0965
Boat	9.3789	7.5503	6.0564	7.6169
Cameraman	8.2121	7.3019	5.6749	7.2723

Table 5. MSE

	EPC	SLILL	SLIA	DLILL
Bird	9589	15965	20973	13169
Lena	9357	13674	18305	13594
Baboon	6993	14413	18575	12368
Einstein	9494	12639	19235	12772
Boat	7503	11438	16394	11375
Cameraman	9709	12162	17687	12291

should be maximized whilst the latter should be minimized. However, the ideal tradeoff between these values is necessary for the method to be used.

3.2.2 Computational Time Analysis

An ideal trade-off between speed (the rate of encryption and decryption for various methods) and security performance, for an encryption engine is a requisite. Though the application domain entirely determines the trade-off, it can be concluded that a system with high security but a less computational (measured in seconds) or the other way round will not be ideal for usage. The computational time analysis for various methods was done on a PC with an 8GB RAM, Intel inside core i5 1.7GHz processor in MATLAB 2013a. Thus, the average time (in sec) for 100 program executions is as deduced from *Table. 6*.

Table 6. Computational Time calculations

Method	Time Elapsed (seconds)
EPC	1.3619
SLILL	0.7656
SLIA	1.6563
DLILL	0.4688

3.2.3 Perception to HVS

A facile speculation on the Table given in section **3.1** can indicate that from the left towards the right end of the Table, for each sample image, the haphazardness increases with respect to the human visual system (HVS). Thus it can be observed that an intra-incremental improvement is depicted in the methods proposed.

4. Conclusion

In this paper, a spectrum of techniques has been proposed to efficiently encrypt images using enhanced Playfair cipher and lifting wavelet transform which enumerates a fusion between the spatial and frequency domain techniques. The obtained metric values, namely, PSNR, MSE, SSIM and correlation coefficient, makes it evident that the introduced methods are effective. In addition, the contour and histogram analysis imply that HVS detection and frequency attacks can be evaded. Based on the internal analysis of the four proposed techniques, the third method has the optimal result set.

5. References

1. Kerckhoffs A. La cryptographie militaire. Journal Des Sciences Militaries. 1883 Jan; 9:5–83.
2. Stallings W. Cryptography and network security: Principles and practice (3rd edition). 3rd ed. United Kingdom: Prentice-Hall, 2002; 1–43.
3. Khalifa A, Atito A. High-capacity DNA-based steganography. 8th International Conference on Informatics and Systems (INFOS), Egypt. 2012.
4. Pradhan C, Saha BJ, Kabi KK, Arun A. Comparative analysis of digital watermarking scheme using enhanced play fair cipher in DCT & DWT. Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT), India. 2014 .
5. Vidya GR, Preetha H, Shilpa GS, Kalpana V. Image Steganography Using Ken Ken Puzzle for Secure Data Hiding. Indian Journal of Science and Technology. 2015; 7(9):1403–13.
6. Wu H, Dugelay JL, Cheung Y. A data mapping method for Steganography and its application to images. Lecture Notes in Computer Science. 2008; 5284:236–50.
7. Swain S, Gandharba G. Digital image steganography using nine-pixel differencing and modified lsb substitution. Indian Journal of Science and Technology. 2015; 7(9):1444–50.
8. Navas KA, Ajay MC, Lekshmi M, Archana TS, Sasikumar M. DWT-DCT-SVD based watermarking. 2008 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE '08), India. 2008.
9. Daubechies I, Sweldens W. Factoring wavelet transforms into lifting steps. The Journal of Fourier Analysis and Applications. 1998 May; 4(3):247–69.
10. Gholipour M. Design and implementation of lifting based integer Wavelet transform for image compression applications. Digital Information and Communication Technology and its Applications. 2011 Jan; 166:161–72.
11. Alam AA, Khalid BS, Salam CM. A modified version of Playfair cipher using 7×4 matrix. International Journal of Computer Theory and Engineering. 2013; 5(4):1–3.

12. Srivastava SS, Gupta N. Optimization and analysis of the extended Playfair cipher. International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), India. 2011.
13. Calderbank AR, Daubechies I, Sweldens W, Yeo B-L. Lossless image compression using integer to integer wavelet transforms. Proceedings of International Conference on Image Processing. 1997; 1:1–4.
14. Jain C, Chaudhary V, Jain K, Karsoliya S. Performance analysis of integer wavelet transform for image compression. 3rd International Conference on Electronics Computer Technology. 2011.
15. Jansen MH, Oonincx PJ. Second generation Wavelets and their applications. United Kingdom: Springer London, 2005.
16. Yongqiang C, Hanping H. Gray image Watermark algorithm in integer Wavelet transform domain. International Conference on Electrical and Control Engineering. 2010.
17. Hemalatha S, Renuka A, Acharya DU, Kamath PR. A secure image steganography technique using integer Wavelet transform. World Congress on Information and Communication Technologies, 2012.
18. Pareek KN. Design and analysis of a novel digital image Encryption scheme. International Journal of Network Security and its Applications. 2012; 4(2):95–108.