

Simple Steganographic Algorithm for Lossless Compression

Lakireddy Bali Reddy College Of Engineering (Autonomous)

M Ravikumar¹, V Phaneendra², G Amarnath³, P Prem kumar⁴, K V Ashok⁵

Asst. Prof

Abstract: Image security has wide applications in data transferring from source to destination system. However, cryptography is a data secrecy technique between sender and receiver, the steganography increases the level of security and acts a protective layer to the hidden information within the source image. In this paper, a compression scheme based image security algorithm for wireless sensor network is proposed to hide a secret color image within the source color image. The main contribution of this paper is to propose a compression scheme which is based on level matrix and integer matrix, and increases the compression level significantly. The performance of the proposed system is evaluated in terms of peak signal to noise ratio (PSNR), mean square error (MSE), number of pixels change rate (NPCR) and unified average changing intensity (UACI). The proposed method achieves 42.65% PSNR, 27.16% MSE, 99.9% NPCR and 30.99% UACI.

Keywords: Image Security, Steganography, Compression, Secret Image, Cryptography

1. INTRODUCTION

Nowadays, lots of information is exchanged through the internet. Security of the information plays an important role in internet to protect the data from the attackers or intruders. Many researchers are using cryptography and steganography for data security over the internet medium. Cryptography deals message encryption but the communication is visible but on the other hand, steganography deals with secret message hiding but the communication is not visible [1].

One of the foremost variations of steganography with cryptography is that encoding the traffic, the communications will be secured but people become aware of the existence of message by observing coded information, although they are not able to realize the message in the data. The steganography technique hides the existence of the message so that intruders cannot detect what communication is going on, thus providing an advanced level of security than cryptography.

Both steganography and cryptography systems are used in providing secret communications almost in a similar approach but vary in terms of methods used to break the system [2].

Steganography methods can be divided into spatial (original) domain methods and transform domain methods. The cover image is initially transformed into frequency domain, and in the next level, the embedding of secret messages into the coefficients of transformed cover image is performed. The steganography algorithms are performed based on various levels of security to produce stego images (stg) with high

imperceptible [3]. These levels are added to be sure that the difficulties to extract the secret image (S) have been accomplished. One more factor that disputes the security level is the amount of payload capacities in the stego image (stg).

Hence, the payload should be calculated cautiously in order to find the maximum number of bits from "S" that can be embedded into a cover image safely and with robustness. Figure 1 illustrates the steganography process where the secret image is embedded into the source image and the secret image is recovered in the receiver side. The main aim of this paper is to apply the compression scheme of image for wireless sensor networks (WSN).

Steganography is the art and science of hiding secret data in plain sight without being noticed within an innocent cover data so that it can be securely transmitted over a network. The word steganography is originally composed of two Greek words steganos and graphia, which means "covered writing". The use of steganography dates back to ancient times where it was used by romans and ancient Egyptians. The interest in modern digital Steganography started by Simmons in 1983 when he presented the problem of two prisoners wishing to escape and being watched by the warden that blocks any suspicious data communicated between them and passes only normal looking one. Any digital file such as image, video, audio, text or IP packets can be used to hide secret message. Generally the file used to hide data is referred to as coverobject and the term stego-object is used for the file containing secret message.

Among all digital file formats available nowadays image files are the most popular cover objects because they are easy to find and have higher degree of distortion tolerance over other types of files with high hiding capacity due to the redundancy of digital information representation of an image data.

There are a number of steganographic schemes that hide secret message in an image file; these schemes can be classified according to the format of the cover image or the method of hiding. We have two popular types of hiding methods; spatial domain embedding and transform domain embedding. The Least Significant Bit (LSB) substitution is an example of spatial domain techniques. The basic idea in LSB is the direct replacement of LSBs of noisy or unused bits of the cover image with the secret message bits. Till now LSB is the most preferred technique used for data hiding because it is simple to implement offers high hiding capacity, and provides a very easy way to control stego-image quality

but it has low robustness to modifications made to the stegoimage such as low pass filtering and compression and also low imperceptibility. Algorithms using LSB in grayscale images can be found.

2. LITERATURE SURVEY

Biham et al. (2005) [1] have utilized Skipjack algorithm for generating block cipher from the image or data in wireless sensor networks. The 80bit key was generated by this algorithm, and it was stable from the attackers. The 64-bit information data was encrypted (encoded) using this secret key. The computations of energy consumptions were done to analyze the suitability of this proposed algorithm for wireless sensor networks.

Biswas et al. (2015) [2] have used Chaotic Map and Genetic Operations for the encryption of data and images. The experiments were conducted using the real-time sensor unit Mica 2 sensor. The number of security mechanisms were analyzed and used in this work to provide confidentiality of the data. A lightweight block cipher algorithm Figure 1. Steganography system. was proposed to secure the data generated by the sensor unit in wireless sensor networks. The authors achieved NPCR about 99.67%, UACI about 33.42% and information entropy about 7.98 for encrypting and decrypting the lena.jpg image.

Bouslimi et al. (2012) [3] have proposed a Joint Encryption scheme for securing the medical images. This method integrated the encryption scheme with watermarking technique to increase the security level of the system. The Advanced Encryption Standard (AES) scheme was used as the encryption process. The authors achieved PSNR about 53.94 dB for ultra sound images and 101.99 dB for PET images.

Ghrare et al. (2009) [4] proposed a matrix based lossless compression technique to compress the medical images. The compression ratio was low due to its lossless technique. Guo et al. (2016) [5] have developed biometric based encryption algorithm. Face and finger print were encrypted using this approach and the private key was generated from master secret key. Guo & Le (2010) [6] have developed JPEG double compression based image security algorithm using compression tables. The authors achieved PSNR about 44.1 dB based on two standard compression tables.

The main limitation of this paper was that it did not support time cost, and as the method was based on lossy compression, the compression ratio value was less. Lim et al. (2013) [7] used biometric discretization method to protect the information against attackers. The Detection Rate Optimized Bit Allocation (DROBA) scheme was applied one of the most effective biometric discretization schemes in this work. The performance of the system was analyzed in terms of false rejection rate and average entropy loss. Ramkumar et al. (2014) [8] developed a image security system which

imposed a binary image into color image using different quantization tables.

This method was not support the imposing a secret color image into source color image. Sahai and Waters (2005) [9] used the fuzzy algorithm for cryptography and private key was generated based on this. This private key decrypt the cipher text using fuzzy logic constructed in encoder side. A private key of identity can decrypt a ciphertext encrypted with another identity, if and only if, the set overlap distance of these two identities. Suzaki et al. (2012) [10] developed an encryption algorithm based on TWINE method. The authors utilized the concept of Feistel technique in this work to generate the cipher text from the plain text. The method stated in this work contained 16 branches and 36 rounds.

Odai M. Al-Shatanawi et al. (2015) [11] proposed Modified Least Significant Bits (MLSB) method to hide the secret image within the source image using the pixels detection in a random manner. The authors were then applied Advanced Encryption Standard (AES) technique on the stego image against from the different attackers.

Shuliang Sun (2015) [12] used Canonical Gray Coding (CGC) technique to hide the information using Bit-Plane Complexity Segmentation (BPCS) steganography method.

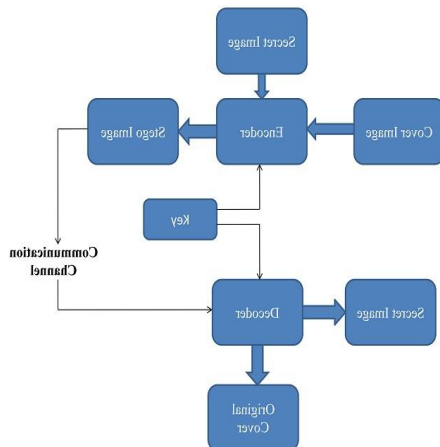
Mandal and Das [13] proposed a steganography method for color images based on difference in pixel values. Secret data was hiding in the component of a pixel in a color image. The attacks on the secured image were not analyzed by the methodologies stated in conventional techniques [1]-[9]. The conventional methods also not discussed and analyzed the embedding of two color images for security purpose.

These limitations are overcome by the methodology proposed in this work. The main contribution of this paper is to provide a novel compression scheme which is based image security algorithm for WSN and it is used to hide a secret color image within the source color image in order to perform both security and compression in WSN applications.

3. PROPOSED METHOD

The proposed methodology for image security system based on compression technique is illustrated in Figure 2. The main principle of this proposed method is to obtain a secured embedded image with high compression ratio and stable to against attackers as shown in Figure 2. The secret color image is block permuted, and the secret key is generated from the block permuted image. This key is used in decoder side to retrieve the secret binary image. The block permuted image is embedded into original source image using block compression table, and the compression technique is applied on this embedded image to produce the compressed patterns.

4. BLOCK DIAGRAM



4.1. Binary Secret Image

The RGB color secret image is initially converted into grey scale image. Each pixel in color image consists of 24 bits resolution and each pixel in grey scale image consists of 8 bit resolution. The grey scale image is further converted into binary secret image based on the dynamic threshold. The dynamic threshold value (T) is determined as,

$$T = [\text{Min}(I) + \text{Max}(I)]/2 \quad (1)$$

where, I represent the grey scale image.

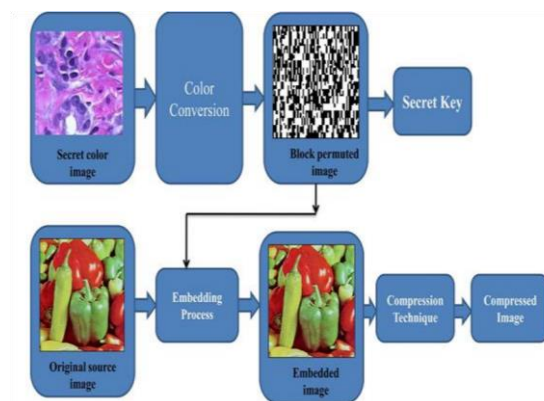


Figure 4.1. Proposed compression based image security system.]

The binary secret image is embedded into the original source image (Ramkumar & Raglend 2014). The width and height of the binary secret image is represented as X*Y. Every pixel in the binary secret image is denoted as P(X, Y). The pixel in this image may have the value either zero or one. Zero represents a black pixel, and one represents a white pixel as depicted in Equation

4.2. Original Source Image

The original source image is denoted as ‘S’ and this image may be either color or grey scale image. The size of this image is represented as M (width) and N (height). The aspect ratio should be verified before embedding the binary secret image into original source image in order to retain the binary secret image correctly. The aspect ratio (Guo & Le 2010) is defined as,

$$P(X, Y) = \begin{cases} 1, & \text{if white pixel} \\ 0, & \text{if black pixel} \end{cases}$$

$$\frac{M}{N} = \frac{X}{Y} \quad (3)$$

In this paper, size of the original source image is 1024×1024 and size of the secret binary image is 128×128 . Then, the aspect ratio is satisfied as,

$$\frac{1024}{1024} = \frac{128}{128} \quad (4)$$

The secret binary image is only embedded into original source image if the aspect ratio is satisfied.

4.3. Block Random Permutation:

Every pixel in the binary secret image has either zero or one. All these values are stored in a matrix called “M”. The number of rows and columns in the matrix is equal to the size of the binary secret image. The size of the shuffling block is denoted as ‘S’ and it may have values one to three, which may be determined randomly. The block random permutation algorithm randomizes the matrix M by dividing M into non-overlapping blocks of the size specified by S, and shuffling these blocks.

The number of elements in S should match the number of dimensions of M, or S can be a scalar specifying an S-by-S-by-S-by-S-by ... block size. “S” should contain positive integers. The size of M in any dimension should be an integer, number of times the specified size of the block in that dimension. The block permuted image is generated by permutation of each pixel block in the secret binary image with a known order. The order of changing the pixel value in the secret binary image is stored as the permutation secret key. This key is

used in the decoder section to depermute the secret binary image in a reverse order. Figure 3(a) shows the binary secret images which have to be embedded into the source image and Figure 3(b) shows the block random permuted images of the corresponding binary secret images.

4.4. Embedding Procedure:

The secret binary image is embedded into original source image using the following procedure.

Step 1: Determine the randomized factor ‘r’ using the size of original source image and secret binary image and it is given as,

$$r = \frac{M}{X} * \frac{N}{Y} \quad . (5)$$

In this paper, the randomized factor is $r = 8 \times 8$. Step 2: The original source image is split into number of blocks of size ‘r’. In this paper, the original source image is split into 16 blocks of size 8×8 (each sub-block size) for the size of original source image 1024×1024 .

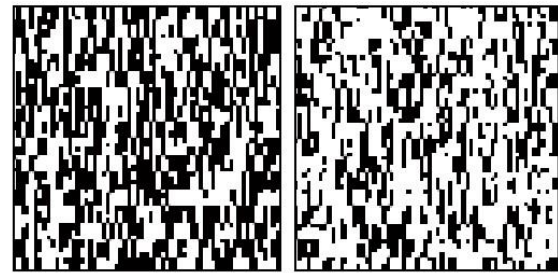
Step 3: Each sub-block in original source image is divided with either compression table 1 (Figure 4) or compression table 2 (Figure 5) (Ramkumar & Raglend 2014) based on the following constraints: (a) (b) (c)



(A)



(B)



(C)

Figure 3. (a) Source color images (babbon, fruits and Lena); (b) Secret binary images “hestain.jpg” and “football.jpg”; and (c) Block random permuted images (after converting binary image).

1	1	2	2	4	4	4	4
2	2	2	2	3	3	3	5
5	2	1	2	3	3	3	3
5	5	5	5	5	1	1	1
2	2	2	2	2	2	3	3
4	4	4	4	2	2	2	2
4	6	6	6	6	7	7	7
7	7	7	1	1	1	1	1

Figure 4. Compression table 1.

1	1	2	2	4	4	4	4
2	2	2	2	3	3	3	5
5	2	1	2	27	22	41	45
6	6	7	7	7	49	51	55
7	7	7	7	55	60	65	67
6	7	6	7	75	75	78	83
5	85	91	95	97	68	76	79
6	91	91	91	96	96	98	99

Figure 5. Compression table 2.

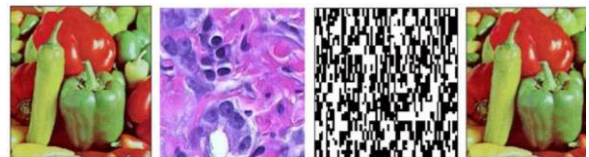


Figure 6. (a) Original source image “fruit.jpg”; (b) Secret color image “hestain.jpg”; (c) Block permuted binary image; (d) Embedded secured image.

$$\text{Secured image} = \begin{cases} \frac{\text{Sub_block}}{QT1}, & \text{if } P(X,Y) = \text{white pixel} \\ \frac{\text{Sub_block}}{QT2}, & \text{if } P(X,Y) = \text{black pixel} \end{cases} \quad . (6)$$

The sub-block of original source image is divided by compression table (CT1) if the first pixel of the secret binary image P(X, Y) is one and CT1 is given as Figure 4. The sub-block of original source image is divided by compression table (CT2) if the first pixel of the secret binary image P(X, Y) is zero and CT2 is given as Figure 5. The secured image is an embedded of the secret color image into original source image. This image is an RGB color image and it is further applied to compression technique to compress this embedded-secured image [14]. Figure 6(a) shows the original source image, Figure 6(b) shows secret binary image, Figure 6(c) shows the block permuted binary image and Figure 6(d) shows the embedded-secured image.

Step 4: The lossless compression technique (JPEG-LS) is applied on the embedded-secured image to generate the compressed patterns. JPEGLS is a lossless/near-lossless compression standard for continuous-tone images [4]. Its official designation is ISO-14495-1/ITU-T.87 [15]. It is a simple and efficient baseline algorithm which consists of two independent and distinct stages called modeling and encoding. JPEG-LS was developed with the aim of providing a low-complexity lossless and near-lossless image compression standard that could offer better compression efficiency than lossless JPEG. It was developed because at the time, the Huffman coding-based JPEG lossless standard and other standards were limited in their compression performance. Total decorrelation cannot be achieved by first order entropy of the prediction residuals employed by these inferior standards.

Step 5: The original secret image is obtained in the receiver section by following the reverse procedure.

5. RESULTS

To validate the effectiveness of the proposed system, we test our proposed image security algorithm on the publicly available open access images. In this paper, “fruit.jpg” and “Lena.jpg” are used as the original RGB source images. The size of the original source image is 512×512 and stored in JPEG format. The secret binary images used in this paper are “hestain.jpg” and “football.jpg” images.

These images are obtained from MATLAB demo toolbox [15] [16]. The size of secret color image is 128×128 . In order to test the robustness of the proposed method, the test source and secret images should have taken from various indoor and outdoor environments. The proposed algorithm is implemented with MATLAB R2014 on a personal computer with Core i3 2.8 GHz CPU and 3 GB RAM. The performance of the proposed system is evaluated in terms of Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) that are described in Biswas et al. (2015).

5.1. PSNR

It indicates the quality of the decoded secret binary image with respect to the original secret binary image. It is expressed as

$$PSNR = 20 \log_{10} \frac{MAX_f}{\sqrt{MSE}} \quad (7)$$

where, MAX f represents the number of pixels in the secret binary image.

5.2. MSE

It indicates the error rate of the decoded secret binary image with respect to the original secret binary image and it is given as,

$$MSE = \frac{1}{X * Y} \sum_0^{m-1} \sum_0^{n-1} \|f(i, j) - g(i, j)\|^2 \quad (8)$$

where, f(i, j) represents the original secret binary image and g(i, j) represents the decoded secret binary image. The width and height of the secret binary image is denoted as X and Y respectively.

5.3. NPCR

It determines the percentage of different pixel numbers between the two images such as original secret binary image and decoded secret binary image. It is expressed as,

$$NPCR = \frac{1}{X * Y} \sum K(i, j). \quad (9)$$

Let $K_{i,j}^1$, (i, j) be the original secret binary image and $K_{i,j}^2$, (i, j) is the decoded secret binary image.

$$k(i, j) = \begin{cases} 1, & \text{if } k1(i, j) \neq k2(i, j) \\ 0, & \text{else} \end{cases} \quad (10)$$

5.4. UACI

It determines the average intensity of differences between the two images such as original secret binary image and decoded secret binary image. It is expressed as,

$$UACI = \frac{1}{X * Y} \sum_0^{m-1} |k1(i, j) - k2(i, j)|. \quad (11)$$

For a better system, the value of UACI should be low, and NPCR should be high. Table 1 shows the performance

Secret color images	PSNR	MSE	NPCR	JACI
testain.jp	1.65	7.16	9.89	1.82
football.jp	2.15	9.75	9.91	0.17
Average.jp g	1.9	8.45	9.90	0.99

analysis of the proposed system in terms of PSNR, MSE, NPCR and UACI. The proposed system achieves the average PSNR about 54.19 dB, MSE about 28.45, NPCR about 99.90 and UACI about 30.99. Table 2 shows the Quantitative analysis with different color channels for different source images and secret images, respectively.

6. CONCLUSION

In this paper, compression based image security for WSN is proposed to increase the level of security from the attackers. The secret binary image is embedded into the original source image using compression technique. This compression technique produces binary and integer matrix which increases the compression ratio of the proposed image security system. The proposed system has high information entropy which indicates the strength of the security system and achieves average PSNR about 41.9 dB and average MSE about 28.45. The methodology in this paper achieves 99.9% of number of pixels change rate (NPCR) and 30.99% of the unified average changing intensity (UACI). In future, this work can be extended to embed the secret video or audio in the source video or audio in WSN to increase the level of security to the next higher level.

7. FUTURE SCOPE

In this work it explores only a small part of the science of steganography. As a new discipline, there is a great deal more research and development to do,

The following section describe areas for research which were offshoots of, or tangential to, our main objectives.

Detecting Steganography in Image Files

Can steganography be detected in images files? This is difficult question. It may be possible to detect a simple Steganographic technique by simple analyzing the low order bits of the image bytes. If the Steganographic algorithm is more complex, however, and spreads the embedded data over the image in random way or encrypts the data before embedding, it may be nearly impossible to detect.

How widespread is the Use of Steganography?

If a technique or set of techniques could be devised to detect steganography, it would be interesting to conduct a survey of images available on the internet to determine if steganography is used, by whom and for what purposes. Steganographic applications are available on the Internet, but it is not known if they are being used.

Steganography on the World Wide Web

The world wide web(www) makes extensive use of inline images. There are literally millions of images on various web pages worldwide. It may be possible to develop an application to serve as a web browser to retrieve data embedded in web page images. This “stego-web” could operate on top of the existing WWW and be a means of covertly disseminating information.

Steganography in printed media.

If the data is embedded in an image, the image printed, then scanned and stored in a file can the embedded data be recovered? This would require a special form of a steganography to which could allow for in accuracies in the printing and scanning equipment.

Anti-steganography measures

As was seen in this thesis, JPEG garbles any unencoded steganographically embedded data. Also, palettization (mapping a large number of colors in an image to a smaller subset of colors) of an image will it unsuitable for steganography. It is likely, as with JPEG, that some means may be employed to prevent loss of steganographically embedded data when its wrapper file is processed. The question remains open as to what is the most effective anti Steganographic tools or set of tools.

8. REFERENCES

- [1] Biham, E., Biryukov, A. and Shamir, A. (2005) Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. *Journal of Cryptology*, **18**, 12-19. <http://dx.doi.org/10.1007/s00145-005-0129-3>
- [2] Biswas, K., Muthukkumarasamy, K. and Singh, K. (2015) An Encryption Scheme Using Chaotic Map and

Genetic Operations for Wireless Sensor Networks. *IEEE Sensors Journal*, **15**, 2801-2809.

[3] Bouslimi, D., Coatrieux, G., Cozic, M. and Roux, C. (2012) A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images. *IEEE Transactions on Information Technology in Biomedicine*, **16**, 891-899.
<http://dx.doi.org/10.1109/TITB.2012.2207730>

[4] Ghrare, S.E., Ali, M.M.A., Jumari, K. and Ismail, M. (2009) An Efficient Low Complexity Lossless Coding Algorithm for Medical Images. *American Journal of Applied Sciences*, **6**, 1502-1508.
<http://dx.doi.org/10.3844/ajassp.2009.15.02.1508>

[5] Guo, F., Susilo, W. and Mu, Y. (2016) Distance-Based Encryption: How to Embed Fuzziness in Biometric-Based Encryption. *IEEE Transactions on Information Forensics and Security*, **11**, 247-257.
<http://dx.doi.org/10.1109/TIFS.2015.2489179>

[6] Guo, J.M. and Le, T.N. (2010) Secret Communication Using JPEG Double Compression. *IEEE Signal Processing Letters*, **17**, 879-882.
<http://dx.doi.org/10.1109/LSP.2010.206>

Random Pixels Selection. *International Journal of Network Security & Its Applications (IJNSA)*, **7**, No. 2.
<http://dx.doi.org/10.5121/ijnsa.2015.7203>

[12] Sun, S.L. (2015) A New Information Hiding Method Based on Improved BPCS Steganography. *Advances in Multimedia*, **2015**, 1-7.
<http://dx.doi.org/10.1155/2015/698492>

[13] Mandal, J.K. and Das, D. (2012) Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain. *International Journal of Information Sciences and Techniques*, **2**, No. 4.
<http://dx.doi.org/10.5121/ijist.2012.2408>

[14] Chang, C., Lin, C. and Fan, Y. (2008) Lossless Data Hiding for Color Images Based on Block Truncation Coding. *Pattern Recognition*, **41**, 2347-2357.
<http://dx.doi.org/10.1016/j.patcog.2007.12.009>

[15] Chen, J., Chen, T.S., Lin, C., Chen, S.Y. and Lin, J. (2015) A Simple JPEG-LS Compressed Technique for 2DGE Image with ROI Emphasis. *The Imaging Science Journal*, **63**, No. 2.
<http://dx.doi.org/10.1179/1743131X14Y0000000086>

[16] El-Emam, N. and Al-Zubidy, R. (2013) New Steganography Algorithm to Conceal a Large Amount of Secret Message Using Hybrid Adaptive Neural Networks with Modified Adaptive Genetic Algorithm. *Journal of Systems*

6110


[7] Lim, M.H., Teoh, A.B.J. and Toh, K.-A. (2013) Dynamic Detection-Rate-Based Bit Allocation with Genuine Interval Concealment for Binary Biometric Representation. *IEEE Transactions on Cybernetics*, **43**, 843-857.
<http://dx.doi.org/10.1109/TSMCB.2012.2217127>

[8] Ramkumar, D. and Raglend, I.J. (2014) Performance Analysis of Image Security Based on Encrypted Hybrid Compression. *American Journal of Applied Sciences*, **11**, 1128-1134.
<http://dx.doi.org/10.3844/ajassp.2014.11.28.1134>

[9] Sahai, A. and Waters, B. (2005) Fuzzy Identity-Based Encryption. In: Cramer, R., Ed., *Advances in Cryptology—EUROCRYPT 2005*, Springer-Verlag, Heidelberg, Germany, 457-473.

[10] Suzaki, T., Minematsu, K., Morioka, S. and Kobayashi, E. (2012) TWINE: A Lightweight Block Cipher for Multiple Platforms. In: Knudsen, L.R. and Wu, H.P., Eds., *Selected Areas in Cryptography*, Springer-Verlag, Berlin, Germany, 339-354.

[11] Al-Shatanawi, O.M. and El Emam, N.N. (2015) A New Image Steganography Algorithm Based on Mlsb Method with *and Software*, **86**, 1465-1481.
<http://dx.doi.org/10.1016/j.jss.2012.12.006>

	M Ravi Kumar, B.Tech ECE, Final Year, Lakireddy Bali Reddy College of Engineering.
	V Phaneendra, B.Tech ECE, Final Year, Lakireddy Bali Reddy College of Engineering.
	G Amarnath, B.Tech ECE, Final Year, Lakireddy Bali Reddy College of Engineering.
	P Prem Kumar, B.Tech ECE, Final Year, Lakireddy Bali Reddy College of Engineering.