International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-5 Issue-3, February 2016

Security Text Massage Verification via Steganography and Color Image in Internet of Things Environment

Haider Sh Hashim

Abstract— Internet of Things (IoT) technologies allow everyday objects including small devices in sensor networks to be capable of connecting to the Internet. Such an innovative technology can lead to positive changes in human life. However, if there is no proper security mechanism, private and sensitive data around humans can be revealed to the public Internet. In this aspect, this paper examines security issues of the IoT that major challenge is faced by IoT. In particular, we focus on the main challenge in exchanging information among devices in IoT's environment. We have combined the concept of attribute based on steganography and crypto hash function to process data with efficient exchange information between two or more entities in the IoT's environment. The proposed scheme has several important security features such as key agreement, resisting malicious attacks, and a good performance. The experimental results view the efficiency and sturdiness of our proposed scheme.

Keywords: (IoT), IoT's, However, performance, experimental, security, resisting

I. INTRODUCTION

The Internet of Things (IoT) is used as an umbrella keyword for covering several appearances related to the expansion of the Internet and the web into the physical kingdom. Now, about two billions persons all over the world are using the Internet for different tasks like (browsing the Web, sending and receiving emails, accessing multimedia content, Services, playing games, using social networking applications and many other tasks)[1].The Information and Communication Technology is bringing up many types progressively things/objects that are attractively establish with sensors and having the capability to communicate with other objects that is transforming the physical world himself into an information and knowledge system. (IoT) qualifies the things/objects in our environment to be lively entrant, i.e., they share information with other stakeholders or members of the network; wired/wireless, frequently using the similar Internet Protocol (IP) that links the Internet. In this technique the things/objects are qualified for acknowledged proceedings and alteration in their surroundings and are expressible and responding autonomously largely without human involvement in an appropriate way [2]. There are a number of bounded security, privateering and trust challenges in the IoT, they all share a number of transversal nonfunctional necessities. Security represents a ticklish element for allowing the extensive fulfillment of the IoT technologies and applications depriving from guarantees in terms of system-level privacy, authenticity and privacy the pertinent stakeholders are improbable to accept IoT solutions on a large measure [3]. Verification considers a riskiness element of security in IoT environment, destination to verify a user's identification when a user desires to need services from provider of IoT. Therefore, any authenticated entities inside IoT needs to check validity each to other for swapping information between them [4]. The emergent possibilities of modern communication need the exceptional way of security especially on IoT. The security of IoT is becoming more important as the number of data being exchanged on the internet increases. Therefore, the confidentiality, verification and authentication are essential to protect data from unauthorized access. This has resulted in an explosive growth of the field of information hiding. Moreover, the information hiding technique could be used extensively on applications of military, commercials, anti-criminal, and so on [5].To protect secret message from being stolen during transmission via IoT, there are two ways to solve this problem in general. First is encryption, which refers to the process of encoding secret information in such a way that only the right person with a right key can decode and recover the original information successfully [6]. Second is Steganography, comes from the Greek word steganos, and means concealed writing. It is an important research subject in the field of cryptography and information security. Steganography hides the secret message into a cover media to generate a stego-media, on which the existence of the embedded secret cannot be detected [7]. Steganography technique can overcomes the conventional cryptographic approach, providing new solutions to secure data transmission without being suspect to censors. The cover media in a steganography scheme could be image, audio, video, document… etc. [8]. However, if the stego-media is lost or corrupted, the secret data cannot be reconstructed. Therefore, several secret sharing techniques have been proposed to overcome this weakness. In this paper, we discuss a secret image sharing scheme with steganography and authentication functions. The cover media in our scheme is a digital image (referred to as cover image), and the image which the secret data is embedded is called as a stego-image. The contributions of our paper: First, the proposed scheme provides verification scheme based on color image and LSB method for hiding information to check verification between set entities in IoT environment. Second, both devices (sender and receiver) in IoT can hide his message authentication code inside color image layers that they used in the verification phase in the more security manner.

Manuscript published on 28 February 2016.
***** Correspondence Author (s)
Haider Sh Hashim, Department of Computer Sciences, Basra University/ Collage of Education & Pure Sciences/ Basra, Iraq.

Third, this scheme can provide strong verification to protect information from malicious attacks. Fourth, this scheme is computationally efficient and Supports simple integration with the available infrastructure, as proven in the experimental results section. The suggested work decreased the cost and increased the information secure, whereas convert massage from explicit text to secure text via depending on hash function MD5 and divided it to three parts and embedded it into three basic layers for original image, this work will be achieved arbitrage between complexity of security and performance, fig 1, [9]. The suggested work achieves good results whereas depending on the most prominent user gauge to make sure from the work abilities, since the experimental results indicate that depending on each of the (PSNR and histogram).The distinctive aspect of the proposed work for the previous methods we've applied in practice through the adoption of the proposed method to work with the IoT environment. By giving permission for somebody to reach important data to another person may be cloud service provider or End user wants to swap his information with another end user inside the IoT environment Both users may be working on Tablet, PCs ,Mobiles and so on. The organization of this paper consists of five sections, the introduction, related works, tools, our propose scheme work, results and conclusion.

II. RELATIVE WORKS

The usage of a stego-key is important, because the security of a protection system should not be based on the secrecy of the algorithms itself instead of the choice of a secret key [9] as shown in Fig. 1. The steganography's job is to make the secretly hidden information difficult to detect given the complete knowledge of the algorithm used to embed the information except the secret embedding key. This so called Kirchhoff's principle is the golden rule of cryptography and is often accepted for Steganography as well [10]. Some steganography methods use a stego-key to embed message for achieving rudimentary security. The other researcher, proposed technique uses predictive position agreed between two parties as stego-key [11]. Same position used only once to enhance security. But drawback of the algorithm is small amount of data to be embedded. The most common and simplest stenographic method is the least significant bit insertion method. It embeds message in the least significant bit. For increasing the embedding capacity two or more bits in each pixel can be used to embed message [12]. At the same time not only the risk of making the embedded statistically detectable increase but also the image fidelity degrades.

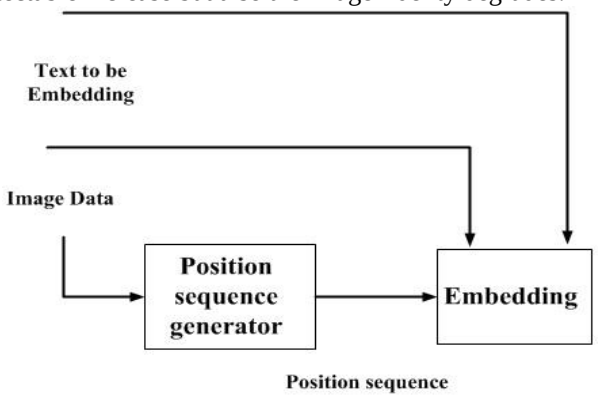

Figure 1. Generalized Stego Key System

So how to decide the number of bits of each pixel used to embed message becomes an important issue of image Steganography. [13]. In [14] authors proposed a method of Multi-Pixel Differencing (MPD) which used more than two pixel to estimate smoothness of each pixel for data embedding and it calculate sum of difference value of four pixels block. Small difference value uses the LSB otherwise and high difference value uses MPD method for data embedding. Their work has been achieved a good results but experimental dataset is too limited. In [15] author proposed another pixel value differentiation method, it used the three pixels for data embedding near the target pixel. It uses simple k-bit LSB method for secret data embedding where number of k-bit is estimated nearly three pixels with high difference value. Retaining better visual quality and high capacity, it simply uses optimal pixel adjustment method on target pixels. Advantage of method is histogram of stego-image and cover-image is almost the same, but dataset for experiments are too small. In [16] authors have introduced a high capacity of hidden data utilizing the LSB and hybrid edge detection scheme. For edge computation two types of canny and fuzzy edges detection method applied and simple LSB substitution is used to embed the hidden data. This scheme is successful to embed data with higher peak signal to noise ratio (PSNR) with normal LSB based embedding.

III. TOOLS

A) Hash function

There are several famous and acknowledged hash algorithms such as Message-Digest algorithm (MD), Message-Digest algorithm 5 (MD5), SHA-0, SHA-1, and RIPEMD-160 in information security fields [17]. Now, we briefly review those hash functions:

1) MD Family: In 1992, Ronald L. Rivest successively presented two hash functions called MD and its revised version named MD5. In cryptography field, MD5 is used hash function based on 12 -bit hash value as output of this function. The input is worked in 512-bit blocks. Additionally, the MD5 function is aimed to be quite fast on 2-bit machines. Furthermore, it does not limit the use of any large substitution tables, here; MD5 have ability to cod quite compactly. MD5 considers slightly more difficult and slower than MD, but it increases the security level in design.

2) SHA Family: The secure hash function (SHA) family is a set of associated with cryptographic hash functions and presented by the National Institute of Standards and Technology (NIST). SHA-0, considers the first member of SHA, was issued in 1993. SHA-1, represents as a developed version of SHA-0, was issued in 1995. Four irregular models have been published by NIST with improved output ranges and a marginally different design as follow: SHA-22, SHA-256, SHA-384, and SHA-512. However, SHA-1 runs on digital message blocks contained 512 bits for a 160-bit digest is produced. SHA-1 is considerably sturdier against malicious attacks [17].

3) Image Authentication Schemes: Authentication considers one of the image security concerns solved by hash function and another problem that is supporting security for illegal processing of digital image is solved by an encryption function.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Image authentication schemes commonly include traditional cryptography, digital signature, fragile and semi-fragile watermarking, and steganography and so on. Any authentication scheme can be aided with the original image to check the validity of user. Image authentication schemes use a crypto-hash function to compute the message authentication code (MAC) based on images. However, the sender generated hash by encrypting message with his secrete key, and then added to the image as an overhead. Additionally, an image hashing procedures are extract a set of distinguished features from the digital image that can be used for authentication process. Hashing function is necessary to prove authentication, content integrity and avoid forgery. An authenticity of image is evaluated by means of digital signature while the image is affected by related distortions. Furthermore, cryptography is very vital to provide secrecy and security to resist. Traditional attacks and other types of attacks when exchange digital images between two entities on the network

B) Least Significant Bit -LSB

A digital image consists of a matrix of color and intensity values. In a typical gray scale image, 8 bits/pixel are used. In a typical full-color image, there are 24 bits/pixel, 8 bits assigned to each color components. The simplest Steganography techniques embed the bits of the message directly into the least significant bit plane of the cover image in a deterministic sequence. Modulating the least significant bit does not result in a human-perceptible difference because the amplitude of the change is small while other techniques "process" the message with a pseudo-random noise sequence before or during insertion into the cover image. The advantage of LSB embedding lies in its simplicity and many techniques use these methods. LSB embedding also allows high perceptual transparency. However, there are many weaknesses when robustness, tamper resistance, and other security issues are considered. LSB encoding is extremely sensitive to any kind of filtering or manipulation of the stego-image. Scaling, rotation, cropping, addition of noise, or lossy compression to the stego-image is very likely to destroy the message. Furthermore an attacker can easily remove the message by removing (zeroing) the entire LSB plane with very little change in the perceptual quality of the modified stego-image [18, 19].

C) Peak Signal to Noise Ratio - PSNR

The Peak Signal to Noise Ratio (PSNR) is the ratio between maximum possible power and corrupting noise that affect representation of image. PSNR is usually expressed as decibel scale. The PSNR is commonly used as measure of quality reconstruction of image. The signal in this case is original data and the noise is the error introduced. High value of PSNR indicates the high quality of image. It is defined via the Mean Square Error (MSE) and corresponding distortion matric, the Peak Signal to Noise Ratio [10]. Here Max is maximum pixel value of image when pixel is represented by using 8 bits per sample. This is 255 bar color image with three RGB value per pixel.

$$PSNR = 10\log_{10}\frac{(L-1)^2}{\frac{1}{N^2}\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}\left[\hat{f}(r,c) - f(r,c)\right]^2} \quad \ldots(1)$$

Where:
L: The number of the gray levels
$f(r,c)$: The original image
$\hat{f}(r,c)$: The reconstructed image

D) RGB Color System

The RGB color system works on the basic principle, that each color is a composition of red, green and blue. Colors are created by adding more light to a starting color of black, and for this reason it is also known as the Additive Color System. Every color in the RGB spectrum is made up of a different value for each of its red, green and blue components. Each of the red, green and blue components is represented by a number in the range 0 to 255. The RGB color system is the most popular systems. It is used to encode the colors. An effective feature is quantization of similar values per element in an image. The output underwater image enhancement in RGB color system not always has improved optimally; Moreover, it has impairment in assimilating rapid brightness impacting. For this reason, we consider transforming an underwater image from RGB color system to HSV color system. Fig.4 shows different types of images.

E) Histogram

A histogram image is the mathematical standard of the digital image. Furthermore, it helps to understand the distribution of the graphic image. The histogram image means the process of distribution density of brightness and the contrast in the gray-level image. This method is applied in our approach as measure, any person can note enhanced ratio during this scale. Fig.7 refers to the image of the histogram method.

IV. OUR PROPOSE SCHEME WORK

The common notations in Table 1, will be used throughout this paper. Our proposed scheme consists of two basic phases: Steganography and Verification. In the Steganography phase, the main components (KM, Sender, Recipient) also uses a cryptographic hash function H(.), The both sender (S) and recipient (R) send their key massages to the Cloud Service Provider (CSP) through a secure channel. We have sets of entities that funding in environment internet of things (IOT), for example mobiles devices (iPhone and so on), tablets devices and computers and others. In this paper we focus in our suggestion work on two basic components sender (S) and (R) that belong to IOT. Both S and R will agree to an identified massage (Key massage) that they use it between them to make the information transmitted securely by using key massage. The functions that are used in this paper are (hash function H ( ) that equal MD5).

A) First phase: Steganography

Steganography is the art of hiding and transmitting message through unsuspecting cover in an effort to conceal the existence of message. The advantage of Steganography is to secretly transmit messages without being discovered. Often, using encryption might identify the sender or recipient as somebody with something to hidden.

S wants to send his text massage to R he will apply the operation by following the steps as below:

1. Select original color image (IM) from his preferred storage.
2. Divide (IM) into the three main layers (R, G, B),

$R = DIV(IM, R)$,
$G = DIV(IM, G)$,
$B = DIV(IM, B)$.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

3. Apply hash function H( ) on his key massage (KM), $MD = H(KM)$

4. Divide MD into three parts based on main layers of color image (see fig.1),

$MDR = COPY(MD, 1,14)$, $MDG = COPY(MD, 15,28)$,

$MDB = COPY(MD, 29,40)$.

$ZAINALABDEEN \rightarrow KM$

Where copy is functioning as copying from message digits (MD) bytes based on the following function,

$copy(Text, Start, End)$

5. HIDE Key massage into color image as follows:

HIDE MDR inside R layer, $Cover\ R = (R, MDR)$,

HIDE MDG inside G layer, $Cover\ G = (R, MDG)$,

HIDE MDB inside B layer, $Cover\ B = (R, MDB)$.

See fig (2).

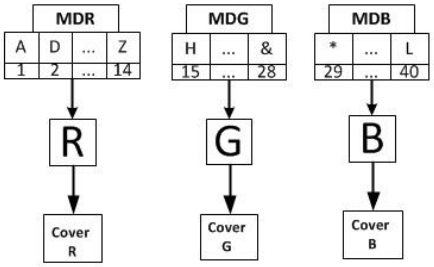

Figure.2. Hidden KM into color image

6. Build cover image as $COVIM = (cover\ R, cover\ G, CoverB)$

7. Sender (S) sends cover image to recipient (R).

$S \rightarrow R : COVIM$

B) Second phase: verification

The verification step is so important in our proposed work to make the recipient of text massage from sender so critical issue in the security if it is not the real end user like (stolen) of data. We will divide this work in this session into four steps to make sure that the text massage i's from the trust sender.

1. Divided cover image (COVIM) into three layers s as follows:

$COVER\ R' = DIV(COVIM, r)$

$COVER\ G' = DIV(COVIM, g)$

$COVER\ B' = DIV(COVIM, b)$.

2. Retrieve information from R' , $COVER\ G'$, $COVER\ B'$ as follows:

$MDR' = Retrieve\ (COVER\ R')$

$MDG' = Retrieve\ (COVER\ G')$

$MDB' = Retrieve\ (COVER\ B')$

3. Collect the key massage KM' fromMDR',MDG', MDB' based on the follows below:

$KMD' = collect(MDR', MDG', MDB)$.

4. R compute the massage digits (hash function) based on his KM, $KMD_R = H(KM)$

Compare $KMD' = KMD_R$, if so, the S is identifier otherwise, the S is not identifier

V. RESULTS

In this section, we conduct several experiments for gauging the efficiency and the effectiveness of our work. Figures (1-5) explains histogram of original, cover images. In addition, Table II, shows the results of PSNR of original and cover images where (p1, p2, and p3) represent PSNR of each layer (R, G, B) of image, respectively. Figures are 6 and 7, show time processing of our proposed scheme.

Figure.3. Verification & Steganography phases

Table I. Notations of our proposed scheme

Symbols	Description
KM	*Key massage*
H(.)	*A cryptographic hash function SHA-1*
S , R	*Sender and recipient*
IM	*Image color*
DIV	*Divided function*
R	*Red image layer*
G	*Green image layer*
B	*Blue image layer*
MD	*Massage digits*
COPY	*Copy function*
HIDE	*Hidden function*
COVIM	*Divide Cover image*
R'	*Red image layer in cover image*
B'	*Green image layer in cover image*
G'	*Blue image layer in cover image*
RETRIEVE	
COLLECT	*Collect function*
KM'	*Collect the key massage*
KMD'	*Key massage digits*
KMD_R	*Compute the massage digits*

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Table II. Crypto Hash Function & PSNR for Test phase

	TEXT	Image	Crypto-hash function					PSNR
1	ZAIN	CBOYS	d	6	..	4	4	68.073
2	ZAINAB	CHOUSE	f	7	..	9	l	71.0795
3	HAIDER SHAKIR HASHIM	LENA	d	b	..	c	9	69.9836
4	MARYA	PEPPER	b	2	..	f	c	72.7574
5	ZAHRAA HAIDER	FRUIT	1	3	..	4	8	70.9888

VI. CONCLUSION

In this paper, we explain the practical method for this sensitive issue via using the steganography, hash function tools to verification on the text massage sending from end user for entering to the cloud provider. We have proposed a newer message authentication code scheme for Internet of Things environment based on crypto-hash function and steganography. Our proposed scheme aims at support more functionality and to resist familiar attacks. These vital merits include (1) the valid user can freely to submit his message; (2) our proposed scheme supports secret MAC. A conclusion section is not required. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions.

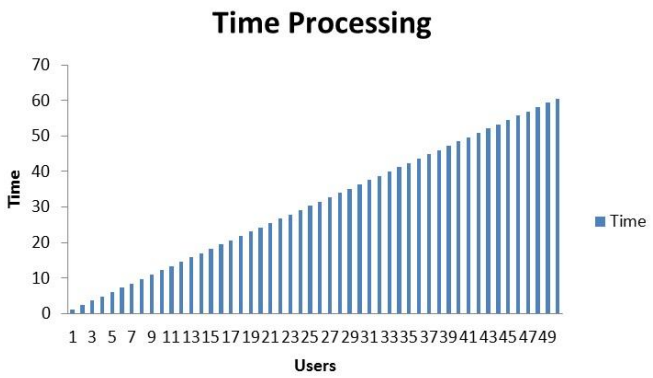

Figure7. Time Processing For Users

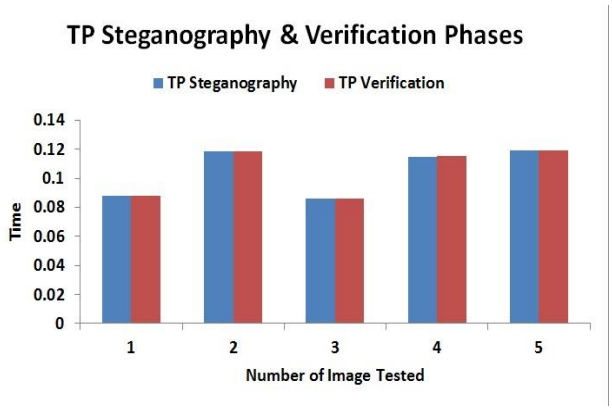

Figure6. Time Processing Steganography & Verification Phases

The fig.1 (a, b) show the original image with its histogram

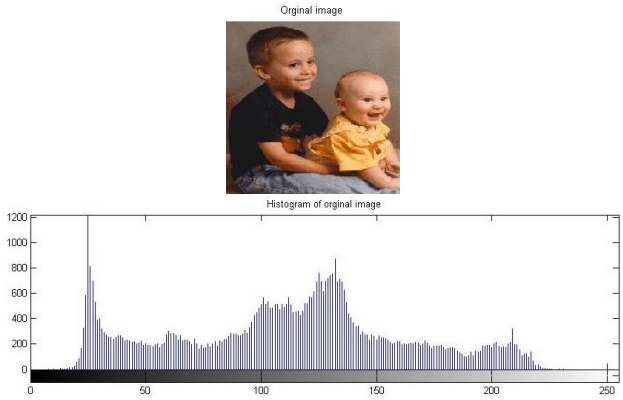

Figure 1.a. Original Image & Histogram of Embedding (Cboys)

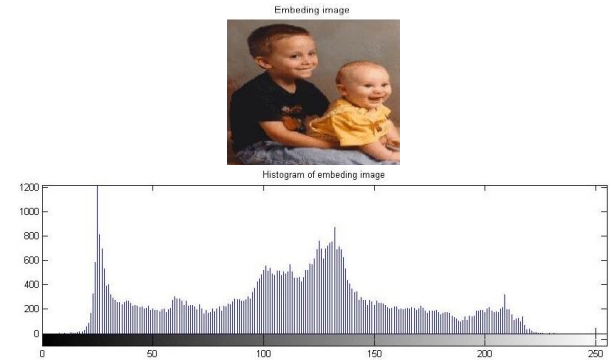

Figure 1.b Embedding Image & Histogram of Embedding (Cboys)

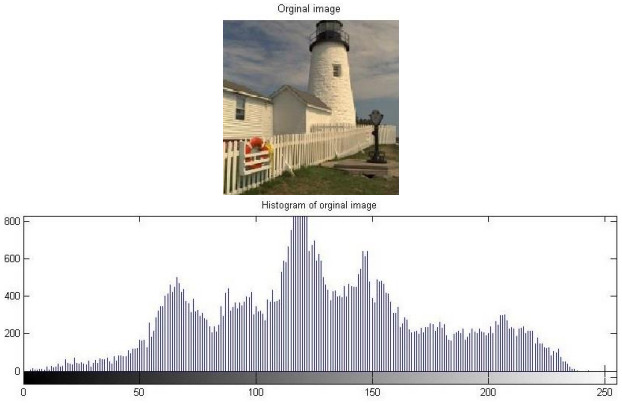

Figure 2.a. Original Image & Histogram of Embedding Image (Chouse)

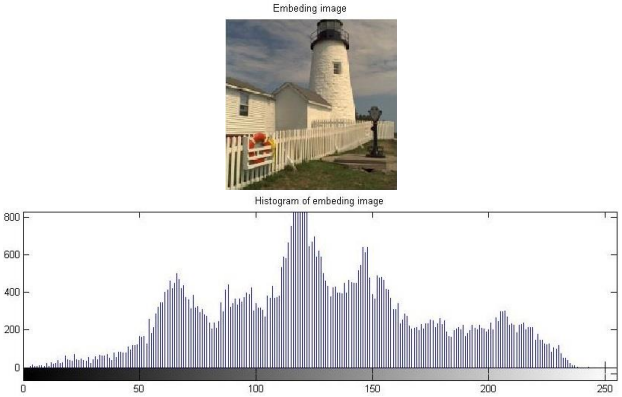

Figure 2.b. Embedding Image & Histogram of Embedding Image (Chouse)

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The fig.3 (a, b) show the embedding image with its histogram

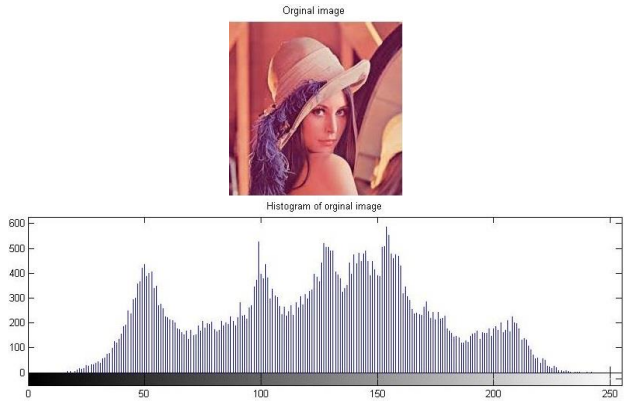

Figure 3.a Original Image & Histogram of Embedding Image (Lena)

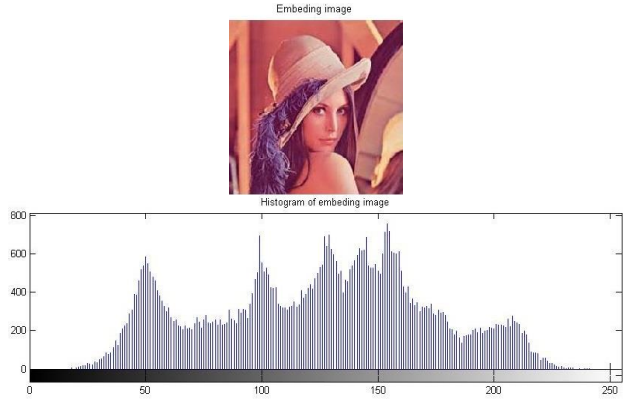

Figure 3.b. Embedding Image & Histogram of Embedding Image (Lena)

The fig.5 (a, b) show the embedding image with its histogram

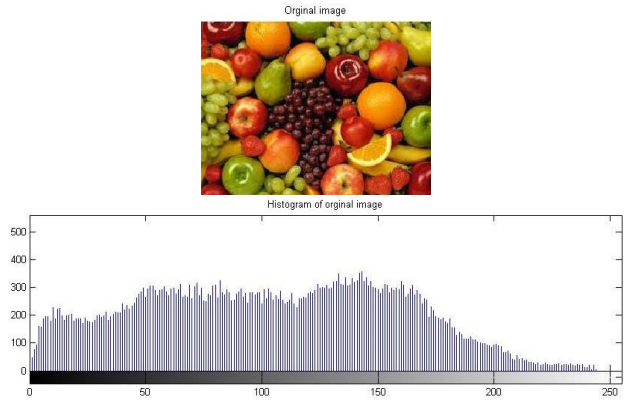

Figure 5.a Original Image & Histogram of Embedding Image (Fruit)

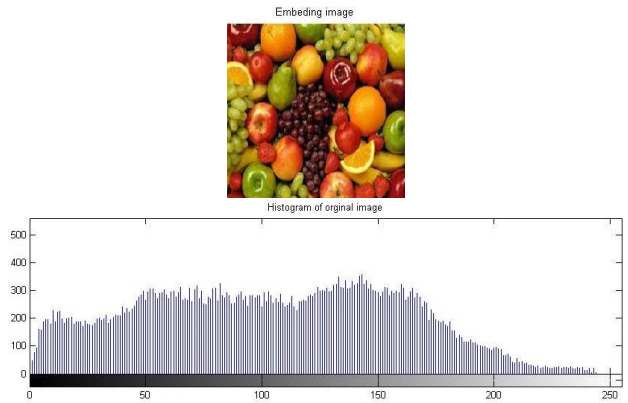

Figure 5.b Embedding Image & Histogram of Embedding Image (Fruit)

The fig.4 (a, b) show the embedding image with its histogram

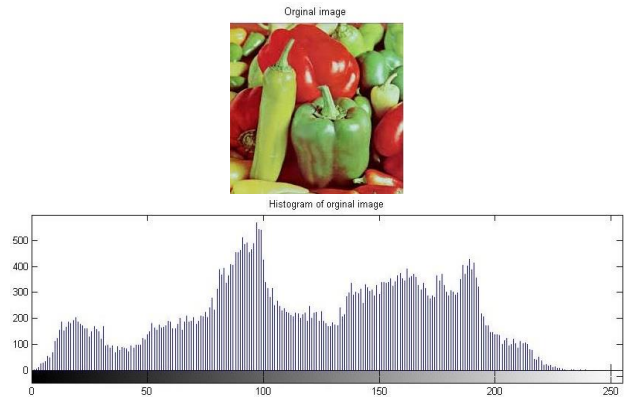

Figure 4.a. Original Image & Histogram of Embedding Image (Pepper)

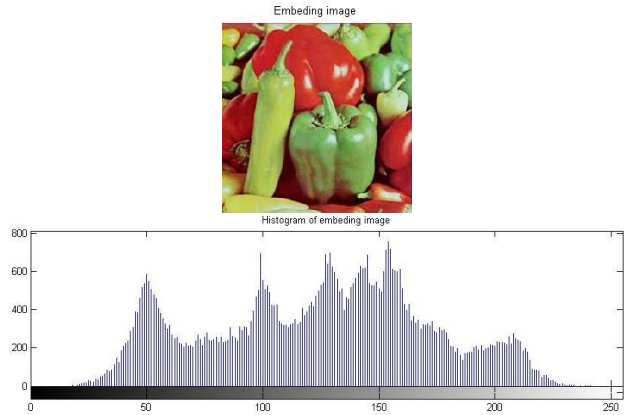

Figure 4.b Embedding Image & Histogram of Embedding Image (Pepper)

REFERENCES

1. D. Miorandi, S. Sicari, F. De Pellegrini, I. Chlamtac," Internet of things: Vision, Applications and research challenges", Ad Hoc Networks vol. 10, issue7, 2012, pp. 1497-1516.
2. K. Ashton, That 'Internet of Things' Thing. RFID Journal, www.rfidjournal.com article print/4986 (2009).
3. J. Buckley (Ed.),"The Internet of things: from RFID to the next-generation pervasive networked systems", Publications, New York, 2006.
4. L. Atzori, A. Iera, G. Morabito, The Internet of Things: a survey, Computer Networks Vol.54, PP. 2787–2805 ,2010.
5. J. Qiu and P. Wang,"An Image Encryption and Authentication Scheme", Proceedings of Seventh International Conf. on Computational Intelligence and Security (CIS), China, pp. 784-787, 2011.
6. H. Sundmaeker, P. Guillemin, P. Friess, S. Woelfflé, Vision and challenges for realising the Internet of Things, Cluster of European Research Projects on the Internet of Things—CERP IoT, 2010.
7. H. Gupta, R. Kumar, S. Changlani, "Enhanced Data Hiding Capacity Using LSB- Based Image Steganography Method", International Journal of Engineering Technology and Advanced Engineering, Vol 3, No.6, 2013.
8. B.Veera, S.M.Verma, C.Uma, "Implementation and Analysis of Email Messages Encryption and Image Steganography Schemes for Image Authentication and Verification ", International Journal of Computer Applications, vol.5, No.5 ,PP.0975 – 8887, 2010.
9. J.Venkata , B.Venkateswara, "Authentication of Secret Information in Image Stenography", IJCSNS International Journal of Computer Science and Network Security, vol.14, No.6, 2014.
10. S.G. Gino, K. Padmaveni, L. Joseph, "Four key Secured Data Transfer Using Steganography and Cryptography", International Journal of Engineering Research and Applications (IJERA), vol. 3, pp.1492-1496, 2013.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

11.K Babu, S. Kumar and A. Babu , “A Survey on Cryptography and Steganography Methods for Information Security ”, International Journal of Computer Applications”, pp. 13-17, vol. 12, no. 2, 2010.
12.R.Amirtharajan, R. Akila, P.Deepikachowdavarapu." A Comparative Analysis of Image Steganography", International Journal of Computer Application, Vol.2, No.3, pp. (0975-8887),2010.
13.A. Cheddad, J. Condell, K. Curran, P.M. Kevitt, "Digital image steganography: survey and analysis of current methods", Signal Processing Vol.90, PP.727–75 ,2010.
14.J. K. Mandal, D. Das,"Image steganographic scheme based on pixel-value differencing and LSB replacement methods". IEEE Proceedings-Vision, Image and Signal Processing, vol. 152, no. 5, PP. 611-615, 2005.
15.Ali A. Yassin, Hikmat Z. Neima, and Haider Sh. Hashim. Security and Integrity of Data in Cloud Computing Based on Feature Extraction of Handwriting Signature, International Journal of Cyber-Security and Digital Forensics (IJCSDF), Vol.3, No.2, pp. 93-105, 2014.
16.S. Mortha, R. Kassey," A High-Capacity Digital Image Data Hiding Scheme Using Adaptive LSB Substitution ", International Journal of Advanced Research in Computer Science and Software Engineering Vol. 2, No. 10, 2012
17.Ali A. Yassin, M. Hasson, H. Ridha, "A New Message Authentication Code Scheme Based on Feature Extraction of Fingerprint in Cloud Computing ", International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 11, 2014.
18.K.-C. Chang, C.-P. Chang, P.-S. Huang, and T.-M. Tu, “A novel image steganography method, IJCSNS International Journal of Computer Science and Network Security, Vol.14 No.6, 2014.
19.M. Juneja, P. S. Sandhu,—Improved LSB based Steganography Techniques for Color Images in Spatial Domain, International Journal of Network Security, vol. 16, No.4, pp. 366-367, 2014.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)