New Efficient and Watermarking Techniques for Security through LSB Substitutions Method

Ashok Choudhary, Anurag Sharma, Gaurav Sharma

***Abstract*— With the speedy development and extensive use of Internet, information communication faces a huge challenge of protection. We require a protected and safe way to convey information. Encryption is a widespread system that is used for encrypting information. Except this for one it is very easy to gain the interest of the attackers because the message cannot be understand directly. The information can be captured, interpreted and yet spread after damage; hence, the reliability of the information is ruined. Digital Watermarking is the method of hiding or embedding an undetectable data into the given data. This undetectable data is called watermark or metadata and the given data is called cover data. Many watermarking algorithms have been proposed in recent years.**

This paper presents a new watermarking technique which is based on least significant bits (LSB) substitution method .our proposed algorithm is improved version LSB substitution method. In this method each cover pixel is used from the spatial domain to the frequency domain. Then, the secret data are embedded into the converted coefficients. as a general rule, methods in the spatial domain get higher hiding capacities but low robustness, and vice versa we used traditional extraction of two shares with separate transparency of secret image for security purpose. We take two different cover images for covering the secret share. Then one secret bit from a secret share is randomly embedded into the ri -th least significant bit (LSBri) of a cover image. Our scheme uses a pseudo random number generator with a secret seed SD to generate a sequence of random numbers {r1, r2…rm}, where m = (2W ×2H) and ri ≤ L. Here, L is the number of least significant bits. we proposed this algorithm for L = 3

***Index Terms*— Steganography, LSB, PSNR and SM**

I. Introduction

Visual cryptograph is a cryptographic technique which allows visual information (such as pictures, text, etc.) To be encrypted in such a way that the decryption can be performed by humans (without computers). Visual cryptography is a cryptographic technique which allows visual information (such as pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by humans (without computers). This era of technology and increasing the wide use of Internet, face a big problem that is security.

Ashok Choudhary (M.Tech) Electronics & Communication Engineering Dept. From Mewar university chittorgarh, Rajasthan .

Anurag Sharma, (M.Tech) Electronics & Communication Engineering Dept. from Gajannath University Jaipur, Rajasthan.

Gaurav Sharma, (M.Tech) Electronics & Communication Engineering Dept. from Gajannath University Jaipur, Rajasthan

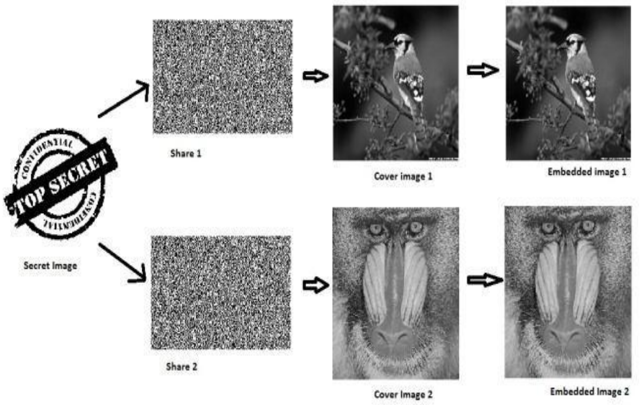

Figure 1: Secret Data Embedding Process using Visual Cryptography.

People need a safe and secured way to transmit information. The one of the best way for secure data communication is Visual cryptography [2]. The first visual cryptographic technique was developed by Moni Naor and Adi Shamir in 1994. It involved breaking up the image into n shares so that only someone with all n shares could decrypt the image by overlaying each of the shares over each other. Practically, this can be done by printing each share on a separate transparency and then placing all of the transparencies on top of each other. In their technique n-1 shares reveals no information about the original image. Visual cryptography technique allows the visual information to be encrypted in such a way that their decryption can be performed by human visual system.
This technique used to encrypt an image into shares such that stacking a sufficient number of shares reveals the secret images. In visual cryptography there are different technique like subpixel, error diffusion, Boolean operation etc.

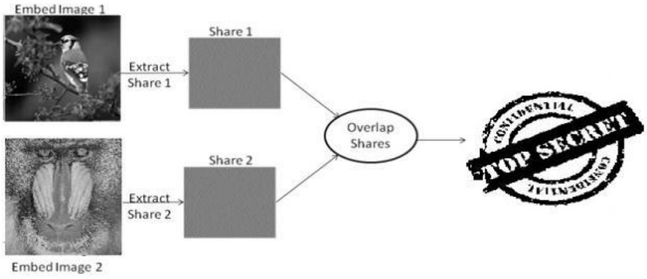

Figure 2: Data Extracting Process using Visual Cryptography.

Visual Cryptography provides information security using simple algorithm. This technique allows visual information to be encrypted using some cryptographic schemes and their decryption can be performed by the human visual systems without any complex cryptographic algorithms. It encrypts the secret image into shares and the stacking of sufficient number of shares reveals the original image. Shares are usually represented in transparencies.

One proposed method is based on improved least significant bits (LSB) substitution algorithms. Methods in the frequency-domain transform each cover pixel from the spatial domain to the frequency domain. Then, the secret data are embedded into the transformed coefficients. In general, methods in the spatial domain get higher hiding capacities but low robustness, and vice versa. Previous image hiding schemes embed the secret into the digital image, and only people with the correct key can extract and decode the secret from the embedding image. If more than one person wants to share the secret, well, previous image hiding schemes cannot do anything about it.

II. THE SCHEME OF IMPROVED LSB ALGORITHM

Research revealed that, the reaction of human eyes to Red, Blue and Green is different. According to the brightness formula: I = 0.3R + 0.59G + 0.11B [5], and the theory of the human visual cells sensitivity of colour, human eyes are most sensitive to the green, the next is to the red, and the least is to the blue [6]. Therefore, the different least bits of brightness components of the red, green, and blue of each pixel can be replaced by the hiding data. And according to the basic principle of the Least Significant Bits Information Hiding algorithm, the effect of replacing the least bit on original data is only 1, the second least bit replacement‟s effect is 2, and the third‟ s is 4, and so on, the nth is 2n−1 .

The higher the bit, the greater effect is. By taking advantage of the less eyesight relevance to the lower bits, the data to be hidden are embedded into the lower (first few least) bits of each pixel.

To begin with, our scheme uses the toral automorphism to mix up all the pixels of the two cover images C1 and C2. Then one secret bit from a secret share is randomly embedded into the ri -th least significant bit (LSBri) of a cover pixel. Our scheme uses a pseudo random number generator with a secret seed SD to generate a sequence of random numbers {r1, r2…rm}, where m = (2W ×2H) and ri ≤ L. Here, L is the number of least significant bits decided by the user. The embedding procedure of Method- 1, when L = 3, is shown in Figure 3.1. For example, if r = 2, then the LSB2 of a cover pixel is replaced with a secret bit

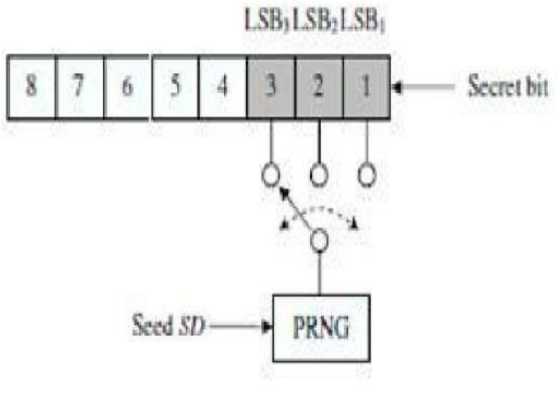

Figure 3: The Embedding system of random bit Replacement

For a gray-level pixel, LSB1, LSB2, and LSB3 are three least significant bits. Although those three bits are changed, the image quality still remains the same. A large value L increases the detect ability but decreases the stego- image quality. To strike a balance between the image qualities and detect ability, setting the L value to be 3 or 4 is appropriate.

III. WATERMARKS ALGORITHMS

Proposed watermarking scheme is defined as 7-tuple (S, S1, S2, C1, C2, E1 and E2): „S‟ denotes the Secret image (which has to be protected). „S1‟ and „S2‟denotes the two different Secret shares of Secret Data.
„C1‟ and „C2‟denotes the two different Cover image for watermarking.

„E1‟ and „E2‟ denotes the two embedded image generated from Embedding Algorithm.

A. Split Secure Data Algorithm

Step 1: Read Input Secure Data „S‟ and Convert it into 256*256 Step 2: Convert Secure Data „S‟ RGB into Binary Image.
Step 3: Initialize Two different Shares with Pixel values Zero Step 4: Find Pixel value one in S and Store required values in each of Share „S1‟.
Step 5: Find Pixel value zero in S and Store required values in each of Share „S2‟.
Step 6: Overlap S1 and S2 (For checking Visual Cryptography).

B. Embedding Algorithm

Step 1: Read Two Cover Images „C1‟ and „C2‟ and Convert into Gray.

Step 2: Check That Shares „S1‟ and „S2‟ are not large for Cover images „C1‟and ‟C2‟.
Step 3: Embed „S1‟ into last three LSB of „C1‟ and Generate E1.

```
Set kk=1
For ii: 1 to height of C1 For jj: 1 to weight of C1 If kk<= size of S1
sum=0; sum=sum+4*s1_vector(kk) kk=kk+1
End

If kk<=size of S1 sum=sum+2*S1_vector(kk) kk=kk+1
End
if kk<=size of S1 sum=sum+1*S1_vector(kk) kk=kk+1
end

if C1(ii,jj)+sum<255
E1(ii,jj)=C1(ii,jj)+sum Else
C1=C1(ii,jj)-sum

End

Else
```

ii=Height of C1 jj=Weight of
C1 End
End

Step 4: Repeat Step 3 for „S2" and „C2" Generate E2

Step 5: Calculate Difference between Embedded image"E1", „E2" and Cover Image "C1" „C2".

Step 6: Calculate PSNR for E1 and E2.

IV. SIMULATION RESULTS AND THEIR ANALYSIS

In our simulation we apply the above algorithm for different images. For this purpose we have used MATLAB software. Peak Signal to Noise Ratio (PSNR) and MSE has been calculated for analysis.

The information hiding includes both information embedding algorithms and information extraction
algorithms. Embedding is an information hiding process, while extraction is the restoration process of secret information. Therefore extraction operation is the inverse operation of embedding operation.

Calculating PSNR using following formula:

$$PSNR\ 10\log_{10} db \frac{255^2}{MSE}$$

The mean square error (MSE) of two images of N x N pixels is defined as:
Where Pij is the original cover image

$$SM \frac{\sum_{i1}^{M}\sum_{j1}^{N} W\ i,j\ W^{*}\ i,j}{\sum_{i1}^{M}\sum_{j1}^{N} W\ i,j^{2} \quad \sum_{i1}^{M}\sum_{j1}^{N} W^{*}_{i,j}{}^{2}}$$

Where W_M is Original Watermark and W_M^* is detected Watermark.

$$MSE \frac{1}{N^2} \sum_{i1}^{N}\sum_{j1}^{N} p_{ij}\ p'_{ij}{}^{2}$$

valueand p_{ij}' is the embedded image pixel value. The higher the pixel value the better the are same. Generally value of SM>.75quality of the reconstructed image.
The similarity factor has value [0,1] calculated If SM = 1 then the embedded watermark and using following equation . If SM = 1 then the embedded watermark and the extracted Watermark

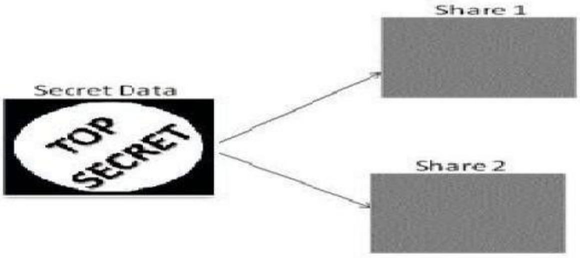

Figure: 4 Share 1 and Share2 from secret.jpg

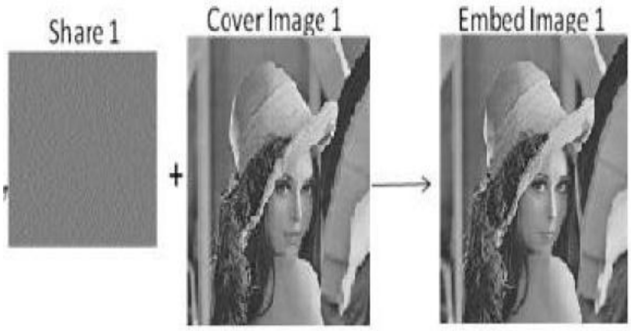

Figure 5: Cover Image and watermarked image for leena.jpg

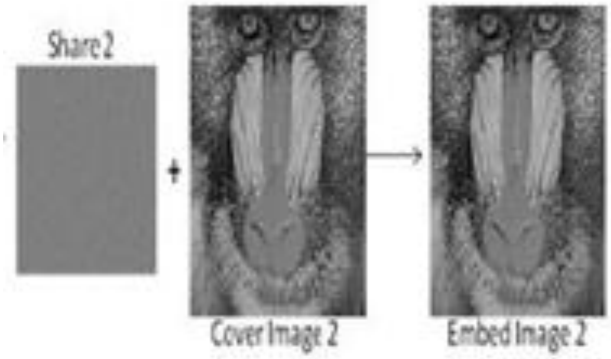

Figure 6: Cover image and Watermarked image for baboons.jpg

		PSNR(with	PSNR(with	MSE
S.No.	IMAGES	Three LSB) (db)	one LSB) (db)	(db)
1	Baboons.jpg	44.15	54.45	0.99
2	Bird.jpg	43.13	51.01	0.99
3	Fruit.jpg	43.88	53.87	0.99
4	Girl.jpg	44.12	51.15	0.97
5	Jnit.jpg	42.92	52.91	0.89
6	Lina.jpg	44.17	51.15	0.73
7	Kids.jpg	45.57	51.51	0.34

Table1: Results for different images

When PSNR is higher than 30, recomposed image has a very good quality and the eye could hardly tell the difference between the original and the recomposed image.

The smaller the PSNR value is, the larger the difference between images will be. The larger PSNR value implies the better image restoration. Usually, when the PSNR value is above 28dB, the image will have good quality of recovery. For the given algorithm, the PSNR value of the original image and the recovered image is 28.7595, which shows that the algorithm proposed in this is effective.

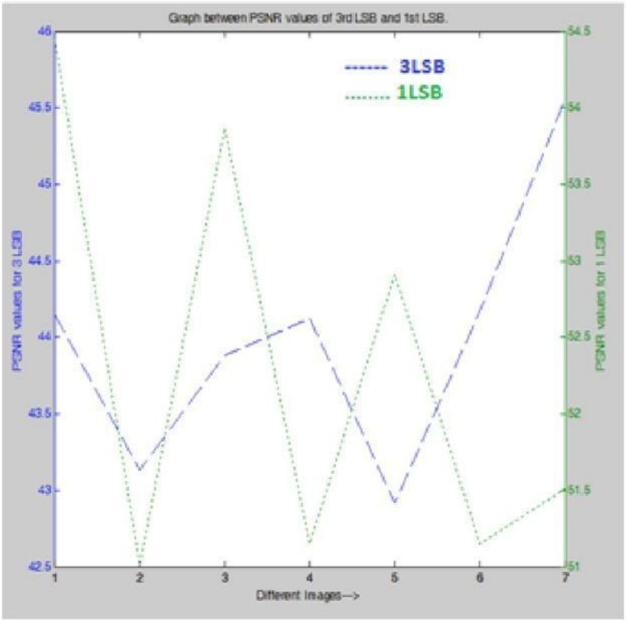

Figure 7: Graph between PSNR value s of different images

The following Table 1 shows the PSNR of the different watermarked images.

V. CONCLUSION

An improved LSB information hiding algorithm is proposed according to human visual theory. The result shows that this new algorithm has many outstanding advantages in the environmental configuration requirement, the time-consuming in running, ease of use and better PSNR value. The information hiding and extraction system implemented on MAT Lab platform takes less running time and recourses and is easy to use.

On the basis of this, we can make following improvements for the LSB algorithm. For example, we could expand the m sequence into 2D and then use corresponding function to improve the detection process; thereby the robustness can be greatly enhanced. In addition, we could integrate the LSB algorithm with some encryption algorithm to improve its security

It provides two levels of security to the information being transmitted. That is the intruders cannot easily break the system. Even if they realize the existence of a secret data they cannot easily recognize the data, since data is hidden in two ways. This system overcomes the demerits of using single level of hiding. That is either using cryptography or steganography and one more thing to add is it requires only the computation time of single level hiding, because visual cryptography requires no computation to decrypt the information.

According to the properties of LSB matching, we find a novel discrimination rule to distinguish the cover and stego images, in which only the least two significant bit planes need to be considered.

VI. SCOPE FOR FUTURE DEVELOPMENT

The proposed algorithm can be implemented in the following area of applications. Future works will aim to achieve better performance and be undetectable by the most famous steganographic analysis, for example, changing bits undisturbed by the concealment of the message.

Pictorial database
Photo image
Video image
Audios

Email server message

REFERENCES

[1] J. R. Hemandez, M. Amado, “DCT domain watermarking techniques for still images as detector performance analysis and a new structure,” in IEEE Transactions on Image Processing, 2000, vol. 9, pp. 55-68.

[2] Lee, G. J., Yoon, E. J. and Yoo, K. Y. (2008), “ A new LSB basedDigital Watermarking Scheme with Random

[3] Mapping Function”, in2008 IEEE DOI 10.1109/UMC.2008.33

[4] S. Z. Yu, “A color image-adptive watermark based on wavelet transform,” in Computer Simulation, 2006, vol. 23, pp. 132-134.

[5] L. Wei, H. T. Lu, F. L. Chung, “Robust digital image watermarking based on sub sampling,” in Applied Mathematics and Computation, 2006, vol. 181, pp. 886-893.

[6] Gil-Je Lee1, Eun-Jun Yoon2, Kee-Young Yoo3 Kyungpoo National University, Buk-gu, Daegu, Republic of Korea vilelkj@infosec.knu.ac.kr, ejyoon@tpic.ac.kr, yook@knu.ac.kr

[7] C. C. Chang, J. Y. Hsiao, and C. S. Chan, “Finding optimal LSB substitution in image hiding by using dynamic programming strategy”, Pattern Recognition, Vol. 36, No.7, 2003, pp.1583–1595.

Ashok Choudhary (M.Tech) Electronics & Communication Engineering Dept. From Mewar university chittorgarh, Rajasthan

Anurag Sharma, (M.Tech) Electronics & Communication Engineering Dept. from Gajannath University Jaipur, Rajasthan.

Gaurav Sharma, (M.Tech) Electronics & Communication Engineering Dept. from Gajannath University Jaipur, Rajasthan