SDEM Based ATM Card Number Hiding Using R-G-B Randomize Key Generator

Bharath K P[1], Shubhratha S[2]

[1] *PG Scholar, Dept. of Telecommunication, SIT, Tumakuru, Karnataka, India,*
[2] *PG Scholar, Dept. of Telecommunication, SIT, Tumakuru, Karnataka, India.*

---***---

Abstract - *In present communication system the lossless data and a security plays an important role. This paper presents a huge amount of data is embedded into cover image without any loss and with high security for an embedded data. The 2 major issues while embedding the data are 1. The first issue is the quality of the image. 2. Second is security for the embedded data.*

In this paper SDEM-DCT (Scramble Data Embedding in Mid-Frequency of DCT) Algorithm which mainly consist of three security levels is used to hide the ATM (Automated Teller Machine) *card number inside a LOGO of the bank. In the first level of security the ATM card numbers (16-digits) of all customers is collected from the main data base file of that bank and then scrambled with R-G-B randomize key generator. In the second level of security the scrambled ATM card numbers are Bit-XOR with secret keys obtained by the R-G-B (Red-Green-Blue) randomize key generator to encrypt the scrambled data and to provide more security. In the third level of security the bank LOGO (cover image) will be divide into 8*8 size of blocks and the encrypted scrambled data of each ATM card numbers will be embedding into the mid-frequency of the DCT(Discrete Cosine Transform) in a diagonal manner. So it ensure that this algorithm provides more security to the ATM card numbers & other large data obtained from the data base file of bank which is embedded in the bank LOGO and also provides more security for many other secret communication or exchanging of bank transaction through internet between banks.*

Key Words: **R-G-B Randomize key generator, Watermarking, Steganography, Bit-reversal, Cover image, Stego Image.**

1. INTRODUCTION

Based on the applications data embedding is divided into two categories according to the relation between cover Image and Embedded information. First category is based on the applications of Steganography. In this technique cover image and embedding message do not have any relationship. Two types of embedding Techniques are.(1)Spatial embedding. In this type of embedding the information are stored into the image pixels starting from least significant Bits (LSBs). (2)Transform embedding – In this method the information is embedded into the cover image after changing the frequency Coefficients. This method is high robust compare to Spatial embedding [2].

The second category is Digital Watermarking. In this method the cover image has a close relationship with embedding message. The embedding message supplies the extra information based on the caption of image, data supplementary about the origin of the image and the authentication of that image etc. But it introduces some noise into the image. This distortion will acceptable only in few applications, but it is not acceptable in many applications. Example, in bank transaction where sender and receiver require same data. All the techniques of data embedding especially in high capacity technique introduce some noise (distortion) into the image and the noise which was introduced is permanent and it won't reversible. But in LSBs technique the noise can be reversible [3].

2. PROPOSED WORK

This paper, introduce a new algorithm on the Transform embedding method with a high robust compare to another method (i.e., Spatial embedding) Fig.1. The proposed algorithm will remove the distortion in spatial embedding method where the information are embedded in the mid frequency of 8*8 DCT matrices and also it has the capacity to store the large amount of ATM card numbers into the cover image with good performance on information hiding and information retrieving.

The proposed algorithm has very less distortion and at the receiver side the retrieved message is same as the hided message into the cover image. It can receive the exact message and the quality of cover image and stego image is same because the data is embedded into the DCT coefficients

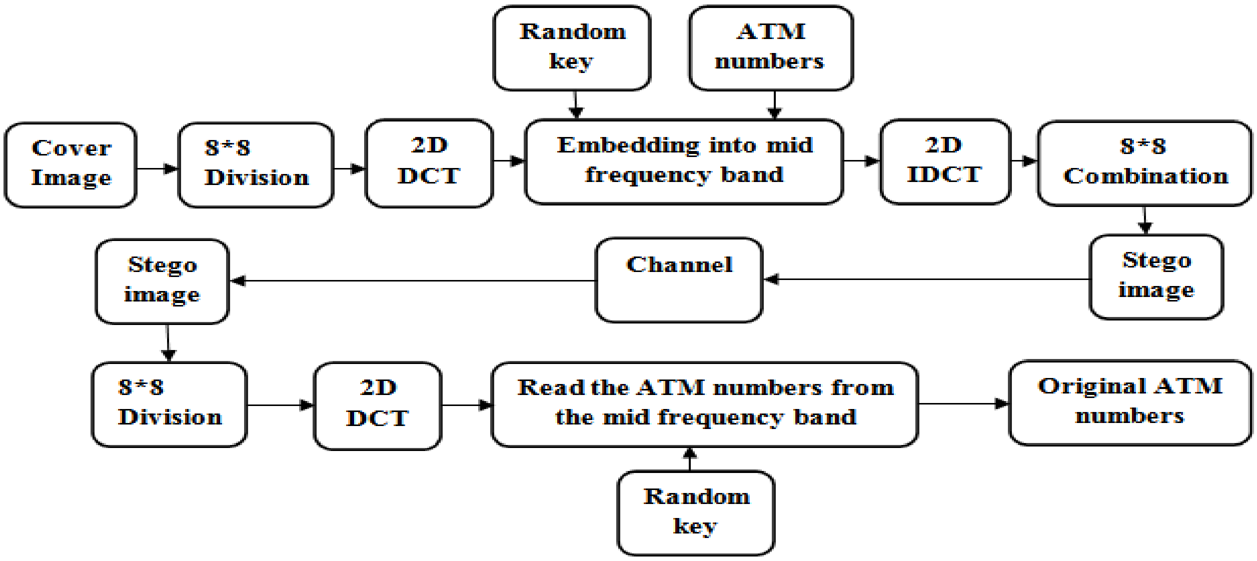

Fig -1: Block diagram of the proposed system.

of cover image[1]. The proposed algorithm uses the cover image of types like BMP,JPEG,GIF,PNG etc.

Procedure for proposed system:

1. Firstly take the logo(cover image) of a bank for the hiding of ATM card number.
2. The logo resolution can be any range, but the range should be divisible by 8. The logo is divided into R-G-B bit plane, each bit plane will be divide into 8*8 matrices.
3. The 8x8 matrix for the entire basic color model is considered and apply DCT2 for each 8*8 matrices.
4. Read the original data which is credit card numbers of the customers.
5. Bit reverse the ATM card numbers.
6. Use R-G-B RANDOMIZE KEY GENERATOR to generate the secret key for the whole process.
7. Apply the bit xor operation to bit reverse numbers with the secret keys, then embed the bit xor operation output in the mid-frequency range of the 8*8 matrices.
8. Convert from frequency to pixel domain by applying IDCT-2.
9. Join all the 8x8 matrix in the raster scan order to get the STEGO image.
10. The STEGO image will be again divided into 8x8 matrices.
11. Apply 2-DCT for every 8*8 matrices, to covert pixel to frequency domain.
13. Read the ATM card numbers from the mid-frequency band.
14. Provide a secret key to read the card numbers.
15. At the final step the original ATM card numbers are Retrieved.

The robust R-G-B key generator algorithm is used for the security purpose, which can generates random. The following steps introduce the algorithm for embedding data into 8*8 blocks with an example.

STEP 1: Original credit card number.

4	2	1	4	5	8	1	8	7	5	0	1	3	7	8	4

STEP 2: Bit reverse of credit card number-security level-1

4	7	5	3	1	0	1	8	2	5	8	7	4	1	8	4

STEP 3: Secret keys generated by R-G-B RANDOMIZE key generator.

5	3	9	13	1	2	1	0	3	11	3	11	12	14	0	2

STEP 4: Bit-XOR the bit-reverse credit card number with secret keys-security level 2.

1	4	12	14	0	2	0	8	1	14	11	12	8	15	8	6

STEP 5: Each bit-xor data will be divided by 1000 , Insert the bit reverse and weighted credit card number into the 8x8 DCT block, as shown in Fig-2.

							0.001
						0.004	0.001
					0.012	0.014	0.006
				0.014	0.011		
			0.000	0.012			
		0.002	0.008				
	0.000	0.015					
0.008	0.008						

Fig -2: Positions of the embedded credit card numbers into single DCT block.

A. Frequency divison in an image:

PURPLE COLOR: This indicates the LOW FREQUENCY range of an image. In low frequency region, it contains highly efficient Information which is clearly visible to the human

eyes, hence by changing the pixels in this portion results in loss of data in the stego image, as shown in Fig-3.
BLUE COLOR: This indicates the HIGH FREQENCY range of an image. In this region, it contains the edge information of an image, modifying which will result in blurring of the edges in the image. Thus we embed the secret data into the mid frequency range of the image, as shown in Fig-3.

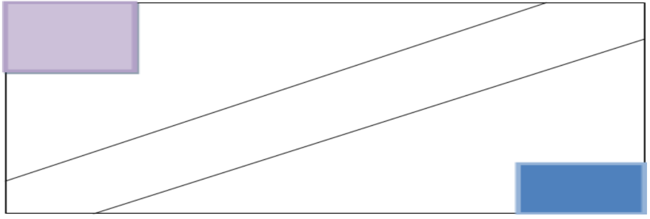

Fig-3: Division of frequency in an image.

The proposed work is explained in the Fig-4. The ATM card numbers are taken from the database of the bank. Each card numbers are encoding with secret keys into the cover image. Now the stego image passes through the communication channel. In the receiver side the ATM card are retrieved by decoding the stego image with same secret keys.

B. Bit reversal order:

In MATLAB the ATM card number data base is generated by using 'RANDINT' function. This data base is imported into the MATLAB using 'IMPORTDATA' function. Bit-reverse and digit-reverse routines are routines in which the data is reordered based on its index value from 0 to N-1, where N is the number of points to be bit/digit-reversed.

C. Extracting Algorithm:

Step-1: By using the **Matlab** program with a command **imread.** Stego image file is divided into 3 planes (Red, Blue, and Green) again each plane is divided into 8*8 blocks.
Step-2: Apply DCT to each 8*8 matrices.
Step-3: Now copy the 16 digits numbers from the each matrix and each digit is multiplied by 1000.
Step-4: In order to retrieve our original data, use bit reverse algorithms and save the values. By Applying IDCT to all 8*8 block and copy the block into the original cover image.
Step-5: Now repeat from step-1 to step-4 get all matrices.

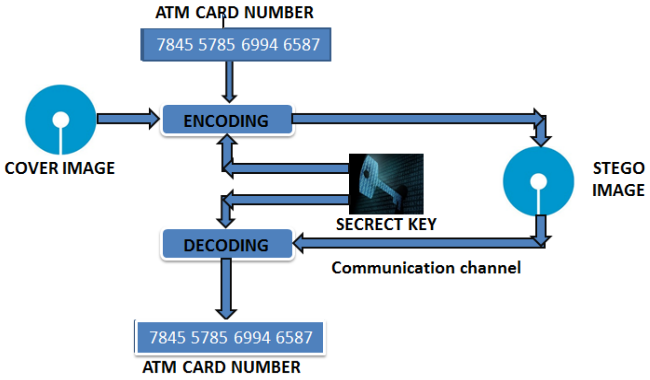

Fig -4: Proposed work explanation.

3. EXPERIMENTAL RESULTS

The experimental results are shown below. In this paper MATLAB Tool is used to develop the algorithms for hiding the data into cover image, Extracting, restoring.

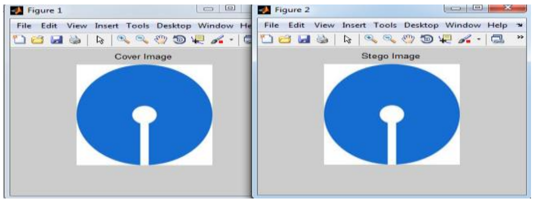
Figure 1
File Edit View Insert Tools Desktop Window He
Cover Image
Figure 2
File Edit View Insert Tools Desktop Window Help
Stego Image

Fig -5: Experimental results for SBI BANK LOGO using DCT.

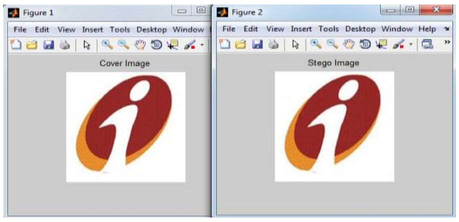
Figure 1
File Edit View Insert Tools Desktop Window
Cover Image
Figure 2
File Edit View Insert Tools Desktop Window Help
Stego Image

Fig -6: Experimental results for ICI BANK LOGO using DCT.

LOGO'S	TRANSFORM	PSNR
SBI bank	DCT	39.5094
	FFT	23.3141
ICI bank	DCT	39.2634
	FFT	27.7060
LENA	DCT	37.7539
	FFT	26.3534
BABOON	DCT	30.3273
	FFT	25.8529

Table 1: Comparison of PSNR for DCT & FFT.

The table 1 shows the PSNR for 4 different logo's, i.e., SBI,ICI, LENA, BABOON . The PSNR for DCT is more compared to FFT. The energy compaction is more in DCT, compared to FFT. Hence the image will get blurred in FFT Compared to DCT. Therefore from the comparison table, it shows that DCT is more efficient in high data transformation compared to FFT.

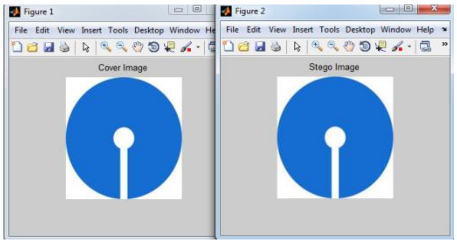

Fig- 7: Experimental results using DCT for SBI BANK LOGO.

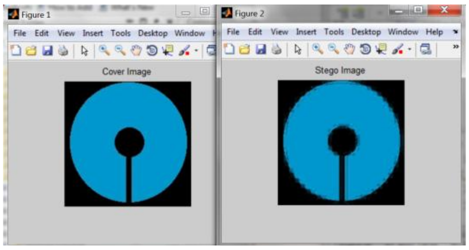

Fig- 8: Experimental results using FFT for SBI BANK LOGO.

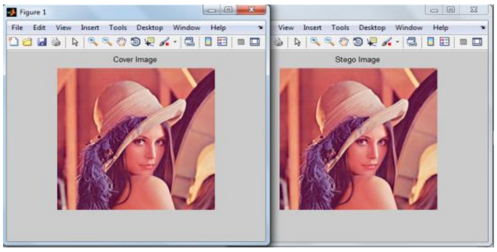

Fig- 9: Experimental results using DCT for LENA IMAGE.

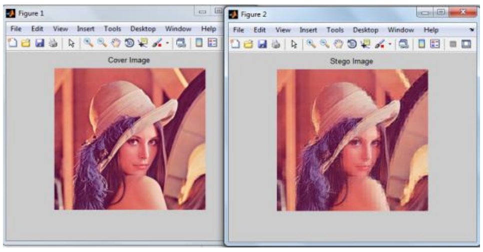

Fig- 10: Experimental results using FFT for LENA IMAGE.

4. CONCLUSION

In this paper, data hiding method with a high capacity algorithm is proposed. By using the proposed algorithm the ATM card numbers are embedded into the cover image. For more security purpose a new algorithm called R-G-B randomize key generator is proposed. This introduces 3 security levels. 1. The data (ATM card numbers) is Bit reversed. 2. The Bit reversed data is XOR with secret keys which is generated by R-G-B randomize key generator. 3. The data is embedded into the DCT blocks.

After the experimental results it shows the proposed algorithm provides the better quality of image and embedding capacity can be varied and also the stego image has very low distortion. The proposed work is well suited for Bank transactions over the internet .In the future work the proposed method can be extends for many DCT levels and also many ATM card numbers digits in a single block and better quality of image with more security levels.

REFERENCES

[1] Dr. Mohammad V. Malakooti, Mehrzad Khederzadeh, “A Lossless Secure Data Embedding in Image Using DCT and Randomize Key Generator”.

[2] Jessica Fridrich*, Miroslav Goljan, Rui Du, “Lossless Data Embedding For All Image Formats”.

[3] Hanizan Shanker Hussain, Syed Ahmad Aljunid, Saadiah Yahya and Fakariah hani Mohd Ali, “A Novel Hybrid Fuzzy SVM Image Steganographic Model”.

[4] Kobayashi, H., Y. Noguchi and H. Kiya (1999). A Method of Embedding binary data into JPEG bitstreams.IEICE Trans. Information and Systems, J83-D-II, 1469–1476.

[5] K. B. Raja, Vikas, Venugopal K. R and L. M. Patnaik, “High Capacity Lossless Secure Image Steganography using Wavelets,”International Conference on Advances Computing and Communications, pp. 230 – 235, 2006.

[6] Kobayashi, H., Y. Noguchi and H. Kiya (1999). A method of embedding binary data into JPEG bit streams. IEICE Trans. Information and Systems, J83-D-II, 1469–1476.

[7] Radovan Ridzon, Dushan Levisky and Tomas Kanocz, “Information Hiding within Still Images Based on the DCT Coefficients Flipping and Encryption,” Fifty Second International Symposium, pp. 147 – 150, September 2010.

[8] Chang, C.C., T.S. Chen and L.Z. Chung (2002). A Steganographic method based upon JPEG and Quantization table modification. Information Sciences, 141, 123–138.