ATIS with SecureComm'13, 26 September 2013, Sydney, Australia

Reversible Data Hiding Scheme based on 3-Least Significant Bits and Mix Column Transform

Wafaa Mustafa Abduallah[1],
Abdul Monem S. Rahma[2], and Al-Sakib Khan Pathan[1]

[1]Department of Computer Science, International Islamic University Malaysia, Kuala Lumpur, Malaysia
[2]Department of Computer Science, University of Technology, Baghdad, Iraq

Presented By: Prof. Jemal Abawajy - Deakin University, Australia

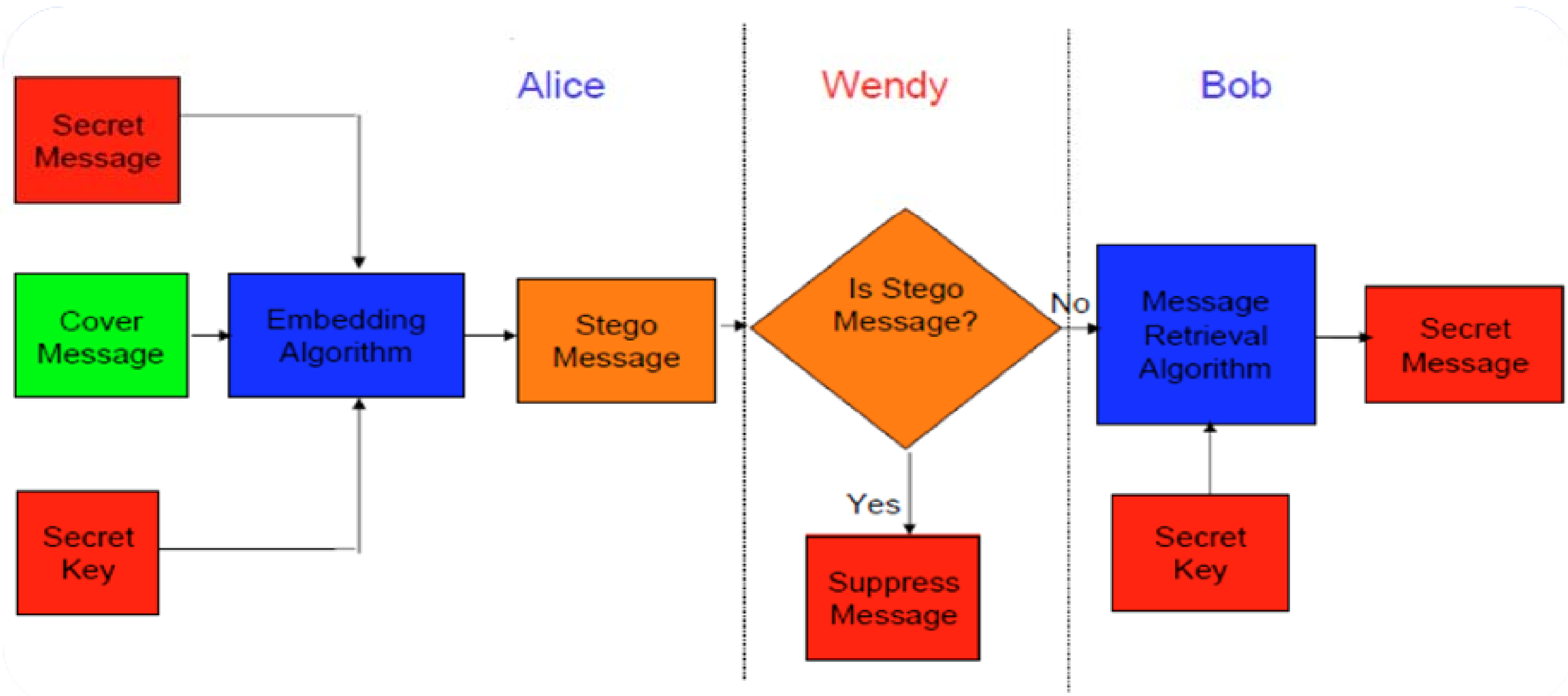
Basic Outline of the Presentation

- Introduction
- Steganography Basics
- Irreducible Polynomial Mathematics
- The Proposed Algorithm
- Experiment Results
- Conclusion
- Future Works

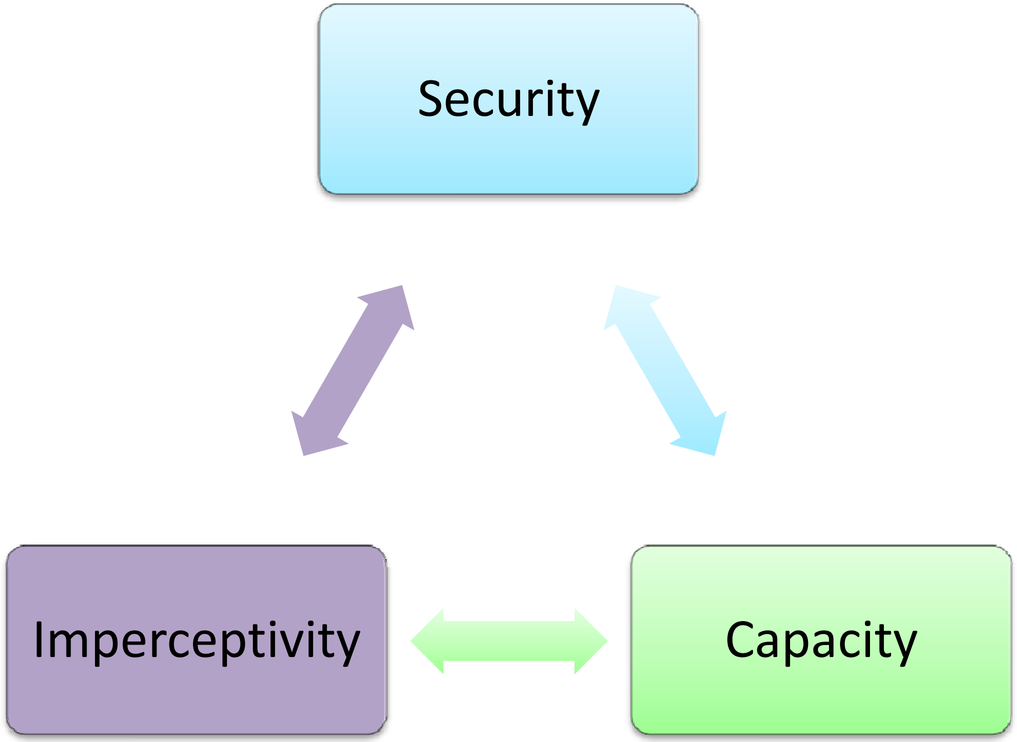
Introduction

- Steganography is the technique of hiding a message in such a way that no one except the intended recipient is aware of its existence.
- A message in *ciphertext*, for instance, might arouse suspicion on the part of the recipient while an *"invisible"* message created with steganographic methods will not.
- The cover media like digital images, audio files, video files, text files, executable files can be used for this purpose.

The Process of Steganography



Steganography Requirement



The performance of a steganographic system can be rated by these 3requirements, which must be as high as possible.

Irreducible Polynomial Mathematics

- In mathematics, a polynomial is said to be irreducible if it cannot be factored into the product of two or more non-trivial polynomials whose coefficients are of a specified type.
- Thus, in the common context of polynomials with rational coefficients, a polynomial is irreducible if it cannot be expressed as the product of two or more such polynomials, each of them having a lower degree than the original one.

Irreducible Polynomial Mathematics

- For example,

  $$(x^2 - 1) = (x - 1)(x + 1)$$

  is reducible over the rationals

- But,

  $$(x^2 + 1)$$

  is not!

The Basic Math. behind This Work

- This work presents a new hiding technique based on the Mathematics of Mix Column Transform.
- The calculations of Mix Column Transform have been done using $GF(2^3)$, which has not been used before in literature. Values in $GF(2^3)$ are 3-bits each, spanning the decimal range [0…7].

The Basic Math. behind This Work

- Multiplication takes place on 3-bit binary values (with modulo 2 addition) and then, the result is computed modulo P(x) [i.e., specific polynomial], which can be:

(1011) = 11 (decimal) or (1101) = 13 (decimal)

The Basic Math. behind This Work

- For example: $5 \times 6 = (101) \times (110) = (11110) = (011) \bmod (1011) = 3$ (highlighted in Table 1) and $5 \times 3 = (101) \times (011) = (1111) = (010) \bmod (1101) = 2$ (highlighted in Table 2).

- Hence, the specific polynomial P(x) provides the modulus for the multiplication results .

The Tables

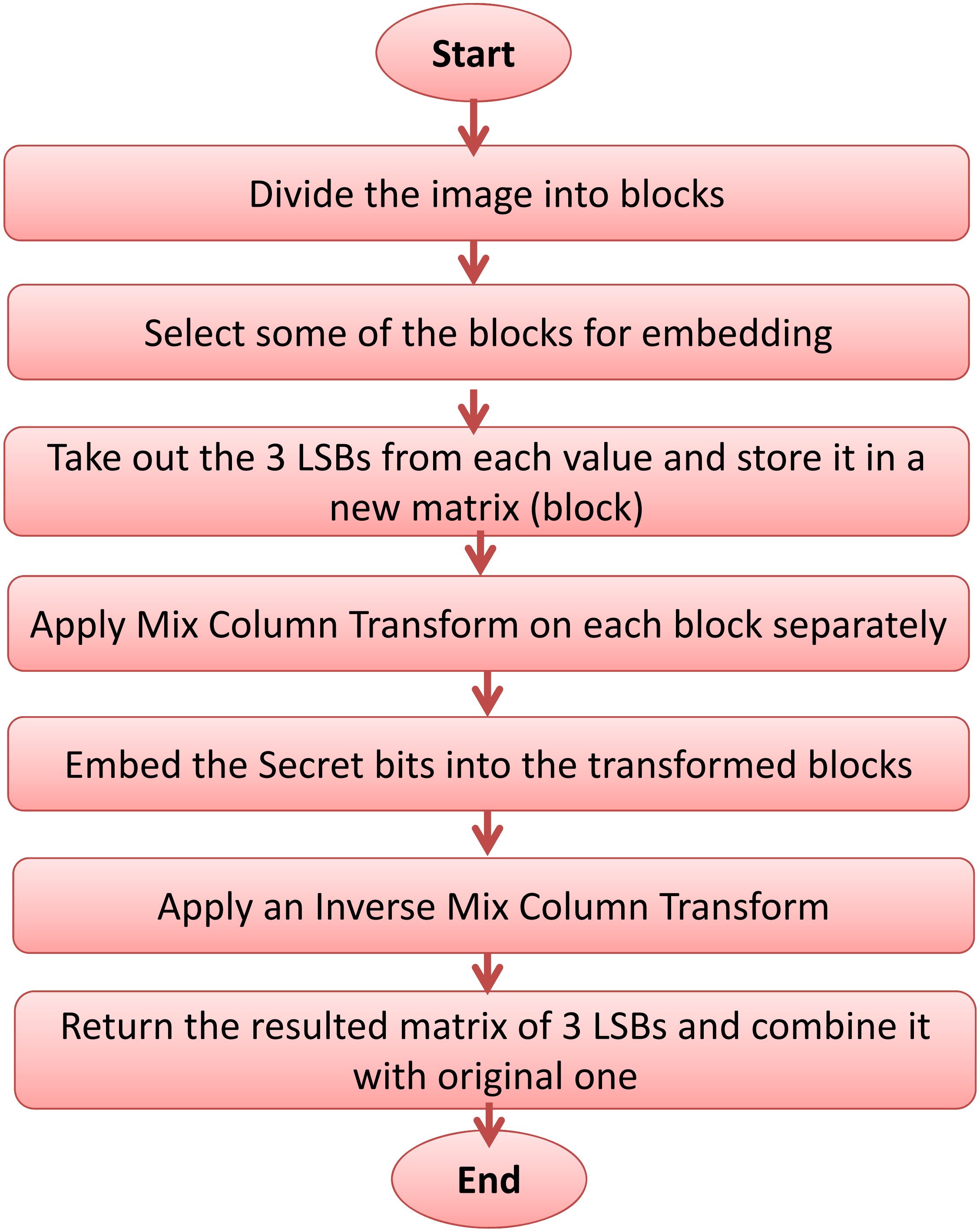
Table 1. Using Primitive Polynomial (11)

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

Table 2. Using Primitive Polynomial (13)

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

Proposed Algorithm



Example of Proposed Transform

Taking a block from an image and preprocessing it before applying the proposed transform:

179	185	177
182	179	180
178	175	185

$$\begin{bmatrix} 10110011 & 10111001 & 10110001 \\ 10110110 & 10110011 & 10110100 \\ 10110010 & 10101111 & 10111001 \end{bmatrix} \rightarrow \begin{bmatrix} 011 & 001 & 001 \\ 110 & 011 & 100 \\ 010 & 111 & 001 \end{bmatrix}$$

Block Matrix

Generating random matrix to be the transform matrix, and finding its inverse to be used in the proposed transform:

07	01	05
01	06	06
05	06	07

$$\rightarrow \begin{bmatrix} 011 & 001 & 001 \\ 110 & 011 & 100 \\ 010 & 111 & 001 \end{bmatrix}$$

Transformed Matrix

05	06	02
06	06	04
02	04	02

$$\rightarrow \begin{bmatrix} 101 & 110 & 010 \\ 110 & 110 & 100 \\ 010 & 100 & 010 \end{bmatrix}$$

Inverse Matrix

Example of Proposed Transform – Ctnd

Converting both matrices to polynomials:

$$\begin{bmatrix} x^2+x+1 & 1 & x^2+1 \\ 1 & x^2+x & x^2+x \\ x^2+1 & x^2+x & x^2+x+1 \end{bmatrix} * \begin{bmatrix} x+1 & 1 & 1 \\ x^2+x & x+1 & x^2 \\ x & x^2+x+1 & 1 \end{bmatrix}$$

Transformed Matrix **Block Matrix**

The Result:

$$\begin{bmatrix} x^2+1 & x & x^2+x \\ x^2+x & x^2 & x \\ x+1 & x^2+x+1 & x^2+x+1 \end{bmatrix} \rightarrow \begin{bmatrix} 101 & 010 & 110 \\ 110 & 100 & 010 \\ 011 & 111 & 111 \end{bmatrix}$$

Having the secret message (111) which can be embedded in the LSB (Least Significant Bit) of the values of the middle column:

$$\begin{bmatrix} 101 & 011 & 110 \\ 110 & 101 & 010 \\ 011 & 111 & 111 \end{bmatrix}$$

Example of Proposed Transform – Ctnd

On the other hand, to get the original values of the block matrix, the resulting matrix from Mix Column Transform should be multiplied by the inverse matrix:

$$\begin{bmatrix} x^2+1 & x^2+x & x \\ x^2+x & x^2+x & x^2 \\ x & x^2 & x \end{bmatrix} * \begin{bmatrix} x^2+1 & x+1 & x^2+x \\ x^2+x & x^2+1 & x \\ x+1 & x^2+x+1 & x^2+x+1 \end{bmatrix}$$

Inverse Matrix **Resulting Matrix**

The Result will be:

$$\begin{bmatrix} x+1 & x & 1 \\ x^2+x & x+1 & x^2 \\ x & 1 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 011 & 010 & 001 \\ 110 & 011 & 100 \\ 010 & 001 & 001 \end{bmatrix} \rightarrow \begin{bmatrix} 03 & 02 & 01 \\ 06 & 03 & 04 \\ 02 & 01 & 01 \end{bmatrix}$$

The Images Used For Experiment

Image 1

Image 2

Image 3

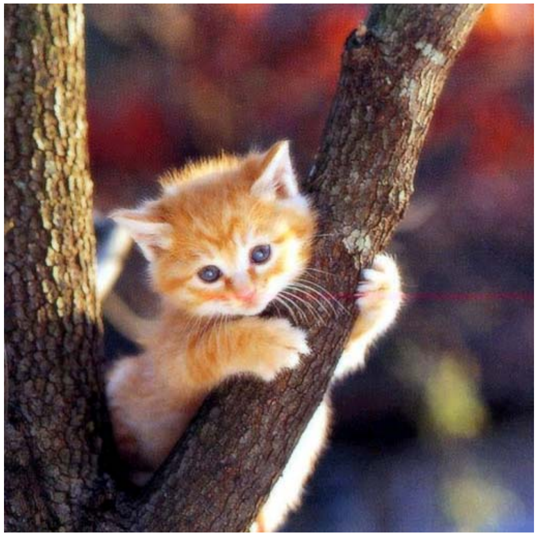
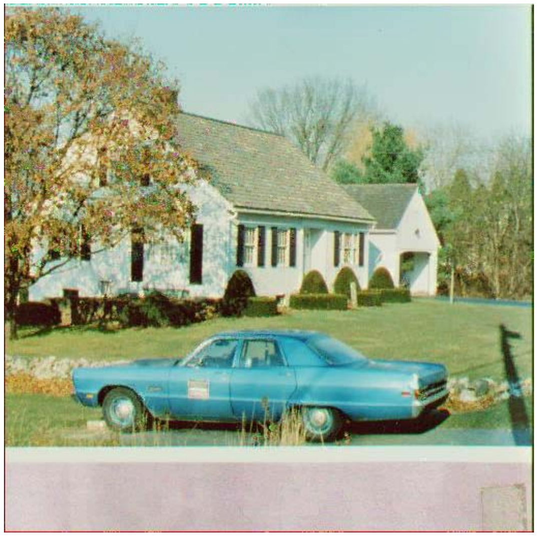


Image 4



Experimental Results & Discussion

- The proposed technique has been tested by using sequence of color images of size (512*512) with JPEG formats. The experiments have been conducted using MATLAB. The image quality of the proposed algorithm has been tested using PSNR, which is estimated in decibel (dB) and is defined as:

$$\mathrm{PSNR} = 10 \log \frac{255^2}{\mathrm{MSE}_{avg}}$$

$$\mathrm{MSE} = \frac{1}{\mathrm{hw}} \sum_{i=1}^{\mathrm{h}} \sum_{j=1}^{\mathrm{w}} (x_{ij} - y_{ij})^2$$

Experimental Results & Discussion

- Another measure for understanding image quality is Mean Structural Similarity (MSSIM) which seems to approximate the perceived visual quality of an image more than PSNR or various other measures.
- MSSIM index takes values in [0,1] and it increases as the quality increases. We calculated it based on the code in (http://www.cns.nyu.edu/~lcv/ssim/) [16] using the default parameters.
- In case of color images, we extended MSSIM with the simplest way: calculating the MSSIM index of each RGB channel and then, taking the average [17].

Experimental Results & Discussion

Table 3. Results of applying the proposed algorithm on the images of size (512*512).

Color Images of size (512*512)	Payload (Bits)	Block Size	PSNR (dB) of the Stego-image	MSSIM	Embedding Duration Time (seconds)
Image1.jpg	452925	4*4	40.3286	0.9522	100.5894
		8*8	40.3497	0.9529	88.5150
Image2.jpg	452925	4*4	41.2353	0.9515	101.0418
		8*8	40.3330	0.9433	88.2186
Image3.jpg	452925	4*4	40.7893	0.9677	100.6362
		8*8	40.3022	0.9644	88.2186
Image4.jpg	452925	4*4	40.7988	0.9733	99.6066
		8*8	40.3466	0.9714	88.3590

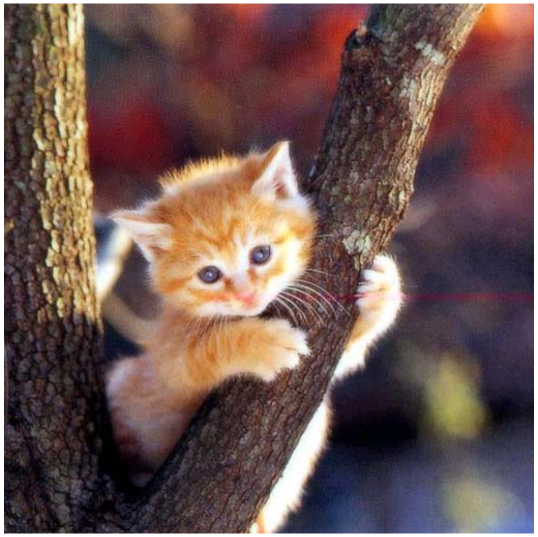
Example Outputs

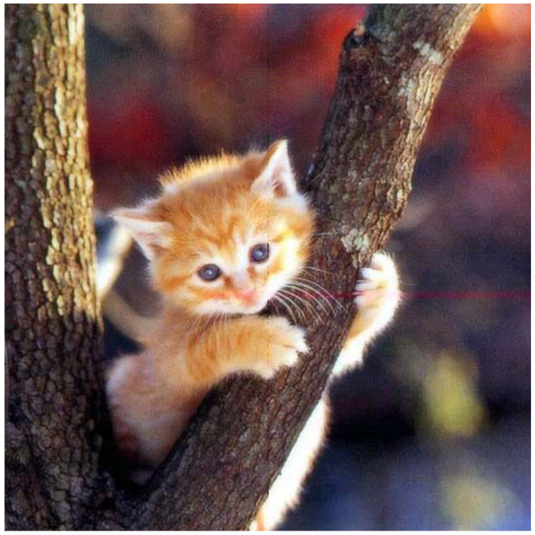
Original Image

Applying on the images of size (512*512) using **block size (4*4)**

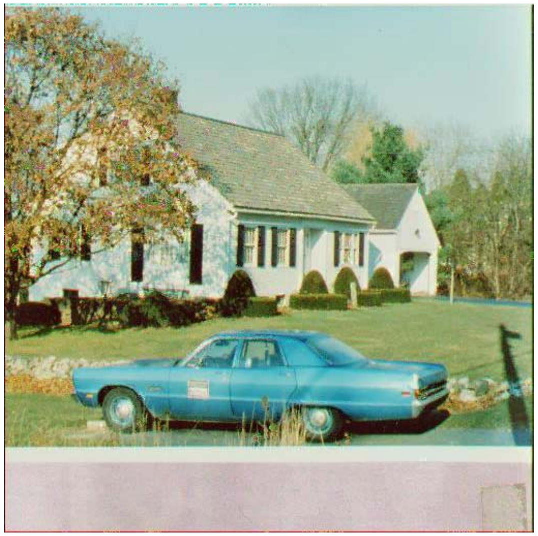
Example Outputs

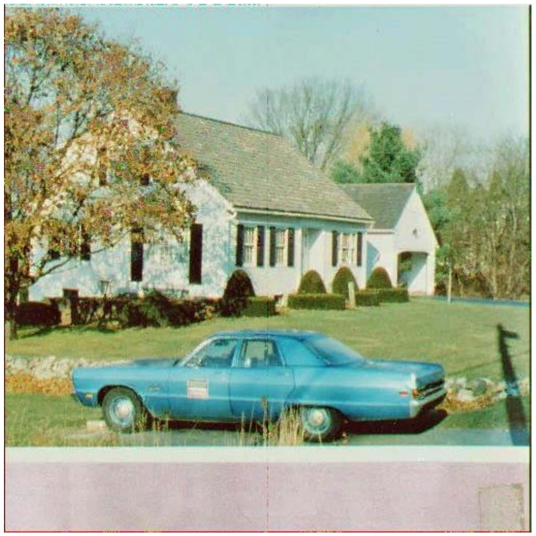
Original Image





Applying on the images of size (512*512) using **block size (8*8)**





Comparative Analysis

- Comparing our proposed scheme with [18] and embedding the same secret message "**AB1001CD**" within the same cover image (baboon.jpg) of size (512*512), we got PSNR=77.3561 while [18] obtained PSNR=72.2156. So, our proposed method beats the scheme used by [18] significantly in terms of imperceptibility through getting higher PSNR.
- On the other hand, when comparing the proposed scheme with its alternative methods that used gray-scale images in their experiments as presented in [10] and [19], our proposed method exceeds those in terms of invisibility as shown the following Table (*keeping the capacities same as were used in those schemes*).

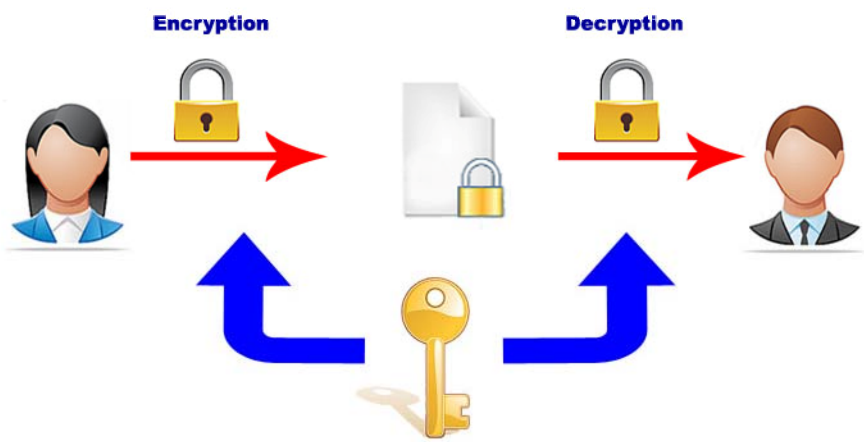
Comparative Analysis

Table 4. Comparison between our proposed method and other related works

The Steganographic Schemes		The Cover Image	Capacity (Bits)	PSNR of the Stego-image in (dB)	Our Proposed Method		
					PSNR of the Stego-image in (dB)	MSSIM Index	Embedding Duration Time in Seconds
1	Reference [10]	Lena .jpg (512*512)	28,001	39.65	47.2571	0.9882	7.6440
2	Reference [19]	baboon .bmp (512*512)	162,775	30.02	40.0453	0.9841	36.4106

Security of the Proposed Method

- According to Kerckhoffs' principle [20], the security of a steganographic system is based on secret key shared between the sender and the receiver called the stego-key and, without this key; the attacker should not be able to extract the secret message.



Security of the Proposed Method

- The secret key was provided in more than one level:
  - The block size is variable and can be any size for instance (3*3), (4*4), etc.
  - The transformed matrix is generated randomly and can be used in our transform if and only if it has inverse.
  - Not all the values of the specified block that have been selected for embedding will be used, instead, only 3 LSBs of each value will be taken out and saved separately in another block to be used in our proposed method which has not been used in the literature before.
  - There is a secret key for selecting the blocks for embedding.

Conclusion

- An efficient steganographic method has been presented – security is increased
- On the other hand, the capacity of embedding secret message has been maximized without affecting the quality of the stego-image as proved by the experimental results.

Future Work

- The robustness of the proposed scheme could be tested against different types of attacks such as the compression to test the efficiency of it and thus, a detailed understanding of the scheme’s practicality could be realized.

References

1. Hernandez-Chamorro, A., Espejel-Trujillo, A., Lopez-Hernandez, J., Nakano-Miyatake, M., and Perez-Meana, H.: A Methodology of Steganalysis for Images. IEEE CONIELECOMP 2009, pp. 102-106, Cholula, Puebla, Mexico (2009).
2. Li, B., He, J., Huang, J., and Shi, Y.Q.: A Survey on Image Steganography and Steganalysis. Journal of Information Hiding and Multimedia Signal Processing, V.2, N.2, 142-172 (2011).
3. Lin, C.-C.: An information hiding scheme with minimal image distortion. Computer Standards & Interfaces, Volume 33, Issue 5, Elsevier, 477–484 (2011).
4. Swain, G. and Lenka, S.K.: A Better RGB Channel Based Image Steganography Technique. CCIS, Volume 270, Springer-Verlag, 470-478 (2012).
5. Swain, G. and Lenka, S.K.: LSB Array Based Image Steganography Technique by Exploring the Four Least Significant Bits. CCIS, Vol. 270, Springer-Verlag, 479-488 (2012).
6. Pandian, N. and Thangavel, R.: A Hybrid Embedded Steganography Technique: Optimum Pixel Method and Matrix Embedding. Proceedings of the International Conference on Advances in Computing, Communications and Informatics, pp. 1123-1130, ACM (2012).
7. Al-Hunaity, M. F., Najim S. A.and El-Emary, I. M.: Colored Digital Image Watermarking using the Wavelet Technique. American Journal of Applied Sciences, 4 (9), 658-662 (2007).
8. Liu, Q.: Steganalysis of DCT-Embedding Based Adaptive Steganography and YASS. The 13th ACM multimedia workshop on Multimedia and security, pp. 77-85, ACM (2011).
9. Rabie, T.: Digital Image Steganography: An FFT Approach. Communications in Computer and Information Science, Volume 294. Springer-Verlag Berlin Heidelberg, 217-230 (2012).
10. Sajedi, H., and Jamzad, M.: Using contourlet transform and cover selection for secure steganography. International Journal of Information Security, Springer, Volume 9, Issue 5, 337–352 (2010).
11. Stallings, W.: Cryptography and Network Security Principles and Practice. USA: Prentice Hall (2006).

References

12. Li, H., and Friggstad, Z.: An Efficient Architecture for the AES Mix Columns Operation. Proceeding of ISCAS 2005, pp. pp. 4637-4640, Kobe, Japan (2005).

13. Addition and Multiplication Tables in Galois Fields GF(2^m), from: http://www.ee.unb.ca/cgi-bin/tervo/galois3.pl [last accessed 30 May, 2013]

14. Yua, Y.-H., Chang, C.-C., and Lin, I.-C.: A new steganographic method for color and grayscale image hiding. Computer Vision and Image Understanding, Volume 107, Issue 3, Elsevier, 183–194 (2007).

15. Wang, Z., Bovik, A.C., Sheikh, H.R., and Simoncelli, E.P.: Image Quality Assessment: From Error Visibility to Structural Similarity. IEEE Transactions on Image Processing, Vol. 13, No. 4, 600-612 (2004).

16. Wang, Z., Bovik, A.C., Sheikh, H.R., and Simoncelli, E.P.: The SSIM Index for Image Quality Assessment, http://www.cns.nyu.edu/~lcv/ssim/ [last accessed: May 19, 2013]

17. Roussos, A. and Maragos, P.: Vector-Valued Image Interpolation by an Anisotropic Diffusion-Projection PDE. Scale Space and Variational Methods in Computer Vision, LNCS, Volume 4485, F. Sgallari, A. Murli, N. Paragios (Eds.) 104-115 (2007).

18. Upreti, K., Verma, K., and Sahoo, A.: Variable Bits Secure System for Color Images. Proceedings of the 2010 Second International Conference on Advances in Computing, Control, and Telecommunication Technologies, pp. 105-107, IEEE (2010).

19. Lee, C.-F., Chen, H.-L., and Tso, H.-K.: Embedding capacity raising in reversible data hiding based on prediction of difference expansion. Journal of Systems and Software, Volume 83, Issue 10, 1864–1872 (2010).

20. Salomon, D.: Coding for Data and Computer Communications. Springer, ISBN-13: 978-0387212456, 2005 edition April 12, p. 345 (2005).

21. MATLAB: The Language of Technical Computing. http://www.mathworks.com/products/matlab/ [last accessed 30 May, 2013]

Thank You

Any query should be directed to: Wafaa Mustafa Abduallah, heevy9@yahoo.com