Open access • Journal Article • DOI:10.5121/IJNSA.2012.4104

Efficient & Secure Data Hiding Using Secret Reference Matrix — Source link

Laxman Tawade, Rajshree Mahajan, Chandan Kulthe

Published on: 31 Jan 2012 - International Journal of Network Security & Its Applications

Topics: Steganography, Information hiding, Cover (telecommunications) and Digital image

Efficient & Secure Data Hiding Using Secret Reference Matrix

Laxman Tawade[1], Rajshree Mahajan[2], Chandan Kulthe[3]
[1]Department of Electronic and Telecommunication Engineering, Pune University, India
[2,3]Aditya Engineering College, Beed, India
tawadelaxman@rediffmail.com

ABSTRACT

Steganography is the science of secret message delivery using cover media. The cover carriers can be image, video, sound or text data. A digital image is a flexible medium used to carry a secret message because the slight modification of a cover image is hard to distinguish by human eyes. The proposed method is inspired from Chang method of Secret Reference Matrix. The data is hidden in 8 bit gray scale image using 256 X 256 matrix which is constructed by using 4 x 4 table with unrepeated digits from 0~15. The proposed method has high hiding capacity, better stego-image quality, requires little calculation and is easy to implement.

.

Keywords:
Discrete cosine transformed (DCT), peak-signal-to-noise-ratio (PSNR), secret reference matrix (SRM)

I. INTRODUCTION

Electronic communication is increasingly susceptible to eavesdropping and malicious interventions. The issues of security and privacy have traditionally been approached by tools from cryptography. Although cryptography techniques can be used to encrypt secret messages for transmission on the internet, the encrypted results can easily arouse attentions of hackers. Steganography embeds secret messages into a cover media without changing the media's perceptual presentation. Thus, when using an image as the cover media, the secret message carried by the stego-image (cover image with embedded secret data) is visually undistorted and avoids attracting the hacker's attention.There are two domains for hiding data in a cover image, namely, frequency and spatial. In frequency domain, secret data can be embedded into the discrete cosine transformed (DCT) coefficients. The advantage of frequency domain embedding is its robustness. When embedding in the DCT's middle to low frequency coefficients, it is generally difficult to destroy the embedded secret without drastically changing the outlook of the cover image. However, the embedding payload is usually lower in the frequency domain in order to maintain the stego-image's visual fidelity and robustness of the hidden data. In spatial domain, the simplest way for embedding is by adjusting the least significant bits (LSBs) of a pixel value in the cover image. The embedding capacity can be very high in spatial domain (up to 30~40% of the cover image's size) and, the embedding and extracting procedure is easy to implement. However, data embedded directly in the LSBs can be easily detected and extracted by internet hackers.

Chang et al. [3] proposed a novel data hiding scheme in spatial domain by using an expansion of Sudoku grid as the map for data embedding and extraction. Chang et al.'s method maintained the high payload approach (hiding capacity is about 19% of the cover image's size) and the hiding security is enhanced compared to traditional LSB substitution based method. Hong et al.[2] directly improved Chang et al.'s method with the stego-image

having a higher PSNR (peak-signal-to-noise-ratio). Further, Chin-Chen Chang et. al. [1] improved Chang et al.'s method and proposed a new spatial domain data hiding scheme by using a secret reference matrix (SRM) for data embedding and extraction. Both Chang et al. and Chin-Chen Chang's methods will be discussed in detail later.

The aim of this paper is to improve the hiding capacity of cover image and increase the complexity to crack the Secret Reference Matrix (SRM). We proposed a new spatial domain data hiding scheme by using a secret reference matrix (SRM) for data embedding and extraction which was inspired from Chin-Chen Chang et. al. [1] Also, the proposed method maintains the feature of higher security than traditional LSB substitution based data hiding scheme and the previously proposed method where the secret reference matrix needs to be kept secret between sender and receiver.

II. RELATED WORKS

Data Hiding Using SRM (Secret Reference Matrix)

In 2009 Chin-Chen Chang et. al. [1] Proposed method in which 256 X 256 matrix is used to map data to embed in cover image and extraction data from stego image. 256 X 256 matrix is formed using 3 X 3 matrix which contain 0 ~ 8 unrepeated digit. The 256 X 256 matrix was constructed because the cover image was only gray scale image. Each pixel value of greyscale is in between 0 to 256.

In the embedding process first secret data is converted into binary data stream which was segmented into N groups and converted into 9 base numeral stream S, where $S = \{d_1, d_2, d_3, \ldots\ldots, d_8\}$, $d_i \in \{0,1,\ldots,8\}$, $1 \le i \le n$ and n is the total number of converted secret digits. For example, a 6-bits binary stream 101100_2 would be converted into two 9-base digits 54_9.Next, given a greyscale cover image $I = \{P_i \mid 0 \le P_i < 256, 0 \le i < (H \times W)\}$, where H and W represented the height and width of the cover image, respectively. Then, every pair of cover pixels (P_i, P_{i+1}) in I, where i is an even integer, $0 \le i < (H \times W)$, is mapped with $M(P_i, P_{i+1})$ onto RM to locate its value x in the corresponding position in the RM. The proposed method to embed the secret digit stream S into I can be described in the following steps.

Step 1: Take the next pixel-pair (P_i, P_{i+1}) out of I and next secret digit dj out of S.

Step 2: If $M(P_i, P_{i+1}) = dj$, let $(P'_i, P'_{i+1}) = (p_i, p_{i+1})$, go to Step 1.

Step 3: Locate the 3×3 table TC for pixel-pair (p_i, p_{i+1}).

Step 4: Sequentially search all pixel-pairs in T^C to find the pixel-pair (P_i, P_{i+1}) with $M(P_i, P_{i+1}) = dj$ (there will be exactly one solution), let $(P'_i, P'_{i+1}) = (P_i, P_{i+1})$, go to Step 1 until all secret digits in S have been embedded.

After the above embedding process, each pixel-pair (P_i, P_{i+1}) in I would find its proper replacement pixel-pair (P_i, P_{i+1}) and the cover image I is converted to the stego image I'. Fig. 1 shows an example to conceal a secret digit 6 into pixel-pair (2, 3). In Fig. 1, since $M(2, 3) = 5 \neq 6$, a 3×3 searching candidate table TC is located and searched. Pixel pair (3, 3) is the only pixel-pair in TC to have M (3, 3) = 6. Hence, pixel-pair (2, 3) is changed to (3, 3) to conceal secret digit 6. The data extraction process of Chang et al.'s method is easy. The data receiver would need the same 256×256 reference matrix (RM) which can be constructed by using 3 X 3 matrix

to extract secret stream S from I'. A pixel-pair in I' (P'_i, P'_{i+1}) can be mapped with $M(P_i, P_{i+1})$ onto RM to discover a 9-base secret digit d_j. The whole secret stream S can then be extracted when all pairs of pixels in I' were mapped. The extracted S is then converted back to its original binary format.

	0	1	2	3	4	5	....	255
0	6	7	4	6	7	4	....	6
1	2	8	3	2	8	3	....	2
2	5	1	0	5	1	0	....	5
3	6	7	4	6	7	4	....	6
4	2	8	3	2	8	3	....	2
5	5	1	0	5	1	0	....	5
...	...	...	...	...	...	...	....	...
255	6	7	4	6	7	4	....	6

Fig. 1: An example of Secret Reference Matrix 256X256 matrix.

	0	1	2	3	4	5	....	255
0	6	7	4	6	7	4	....	6
1	2	8	3	2	8	3	....	2
2	5	1	0	5	1	0	....	5
3	6	7	4	6	7	4	....	6
4	2	8	3	2	8	3	....	2
5	5	1	0	5	1	0	....	5
...	...	...	...	...	...	...	....	...
255	6	7	4	6	7	4	....	6

Fig. 2: The searching area T^C in SRM for pixel-pair (2, 3).

III. Secure Data Hiding Using Secret Reference Matrix

3.1 Construction of SRM

The proposed method was inspired from Chi-Nan Lin et al.'s method. 256×256 Secret Reference Matrix (SRM) is constructed to guide the data embedding and extraction process. The goal is to construct an SRM which can always give a very good replacement pixel-pair (P'_i, P'_{i+1}) for each pixel-pair (P_i, P_{i+1}) in the cover image *I* to conceal secret message *S*. Given a 4×4 table T which was filled with 0~15 unrepeated numerical digits.

Step 1: Position table T at column 0, row 0 of an empty 256 X 256 SRM.

Step 2: Replicate one column at a time horizontally up to 256th column of 256 X 256 SRM.

Step 3: Replicate one row at a time vertically from 5 th row up to 256th row of 256 X 256 SRM.

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

Fig. 3: An example of T (4 X 4 matrix).

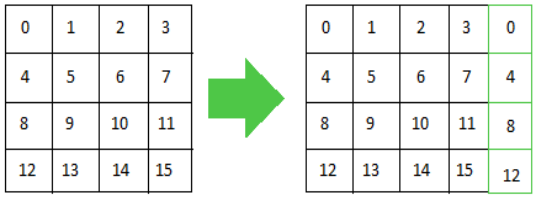

Fig. 4(a): Replicate horizontally.

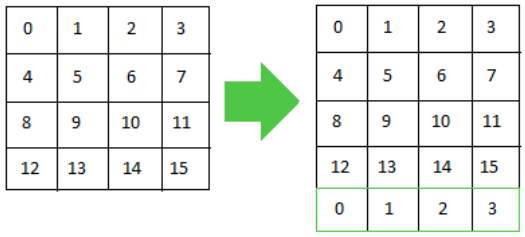

Fig. 4(b): Replicate vertically.

	0	1	2	3	4	5	6	7	....	255
0	0	1	2	3	0	1	2	3	....	3
1	4	5	6	7	4	5	6	7	....	7
2	8	9	10	11	8	9	10	11	....	11
3	12	13	14	15	12	13	14	15	....	15
4	0	1	2	3	0	1	2	3	....	3
5	4	5	6	7	4	5	6	7	....	7
6	8	9	10	11	8	9	10	11	....	11
7	12	13	14	15	12	13	14	15	....	15
....	....	....	....	....	....	....	....	....	....	....
255	12	13	14	15	12	13	14	15	....	15

Fig. 5: An example secret reference matrix (SRM) of dimension 256×256.

Since SRM is constructed using 4 X 4 matrix. There can be 16! (2092278988800) Different possible solutions for the SRM which can enhance the data embedding security compared to traditional simple LSB substitution based methods

3.2 Formation 16 (hexa decimal) base numeral system.

Step 1) Take the secret data from user.
Step 2) Convert it into ASCII format.
Step 3) Convert ASCII to Hexa-decimal.
Eg. Secret data - 'paraj'
ASCII format – 112 97 114 97 106
Binary Format:
0111000001100001011100100110000101101010
Hexa-decimal Format - '706172613A'

3.3 Data Embedding Process

Let $I = \{P_i \mid 0 \le P_i < 256, 0 \le i < (H \times W)\}$ be the gray-scale cover image, where H and W are the height and width of I, respectively. The binary secret data stream is also transformed into hexadecimal digit stream *S*. Let T^C be a 4×4 table in SRM where the centre point in T^C has a minimum Euclidean distance to a pixel-pair (P_i, P_{i+1}) in I. The proposed method to embed the secret digit stream *S* into *I* can be described in the following steps.

Step 1: Take the next pixel-pair (P_i, P_{i+1}) out of *I* and next secret digit *dj* out of *S*.

Step 2: If $M(P_i, P_{i+1}) = dj$, let $(P'_i, P'_{i+1}) = (P_i, P_{i+1})$, go to Step 1.If *dj* is greater or equal than A in hexadecimal format then consider decimal value for locating in T^C. Let digit is *dj* = A; then consider *dj*= 10.

Step 3: Locate the 4×4 table T^C for pixel-pair (P_i, P_{i+1}).

Step 4: Sequentially search all pixel-pairs in T^C to find the pixel-pair (P_i, P_{i+1}) with $M(P_i, P_{i+1}) = d_j$ (there will be exactly one solution), let $(P'_i, P'_{i+1}) = (P_i, P_{i+1})$, go to Step 1 until all secret digits in S have been embedded.

After the above embedding process, each pixel-pair (P_i, P_{i+1}) in *I* would find its proper replacement pixel-pair (P'_i, P'_{i+1}) and the cover image I is converted to the stego image I'. Fig. 6 show an example to conceal a secret digit C (Hexadecimal) into pixel-pair (3, 4). In Fig. 6, since M (3, 4) = 12 ≠ 14, a 4×4 searching candidate table $T^C$is located and searched. Pixel pair (3, 6) is the only pixel-pair in $T^C$to have M (3,6) = 14 = C
(Hexadecimal). Hence, pixel-pair (3, 4) is changed to (3, 6) to conceal secret digit C.

	0	1	2	3	4	5	6	7	....	255
0	0	1	2	3	0	1	2	3	....	3
1	4	5	6	7	4	5	6	7	....	7
2	8	9	10	11	8	9	10	11	....	11
3	12	13	14	15	12	13	14	15	....	15
4	0	1	2	3	0	1	2	3	....	3
5	4	5	6	7	4	5	6	7	....	7
6	8	9	10	11	8	9	10	11	....	11
7	12	13	14	15	12	13	14	15	....	15
....	....	....	....	....	....	....	....	....	....	....
255	12	13	14	15	12	13	14	15	....	15

Fig. 6: The searching area T^C in SRM for pixel-pair (3, 4).

3.4 Data Extraction Process

The data extraction process will be exactly the same as in Chang et al.'s method but will use our newly created SRM as the guiding map for extracting the hexadecimal secret stream S. The same SRM as in the data embedding process can be constructed by using the same 4 X 4 matrix. Each pixel-pair $\left(P'_i, P'_{i+1}\right)$ in I' is mapped to the SRM through $M\left(P'_i, P'_{i+1}\right)$ to get a secret Hexa-decimal numeral d_j. When all hexadecimal digits were recovered, the secret stream S is then converted back to its original ASCII and then to given text.

IV. EXPERIMENTAL RESULTS

To show the experimental result we have used gray scale images: Lena, Baboon, Charlie, Colorize as test images. PSNR values are calculated to show the distortion in the stego image. Comparisons are made with the Chi-Nan Lin etal's[1] method. PSNR is as defined as follows.

$$PSNR = 10\log_{10}\frac{255^2}{MSE}(dB)$$

Where $MSE = \frac{1}{H \times W}\sum_{i=1}^{H}\sum_{j=1}^{W}(p_{ij} - p'_{ij})^2$ represents the mean square error, H represents height and W represents the width of the image, p_{ij} and p'_{ij} are the pixel values of image before and after the embedding of secret data. A higher PSNR value represents lower distortion of image. The hiding Capacity C is measured as bits per pixel (bpp) which is calculated as follows:

$$C = \frac{B}{H \times W}(bpp)$$

Cover Images	Size of Image	Chi-Nan Lin et al's		Proposed Method	
		PSNR	C	PSNR	C
Lena	512X512	67.35	1.58	64.58	2
Baboon	298X298	62.58	1.58	60.22	2
Charlie	512X619	68.19	1.58	67.53	2
Rubik	435X435	65.51	1.58	64.56	2

The Chi-Nan Lin etal's method used one pixel pair to conceal a 9-base secret digit, the hiding capacity equals to 1.58 bpp. In proposed method we are hiding 4-bits in one pixel pair so hiding capacity is 2 bpp. The Stego image quality in terms of PSNR values are shown in table 1. Average PSNR value of Chi-Nan Lin is 65.90 dB and for proposed method is 64.22 dB.The proposed method uses reference matrix(4x4) to guide embedding and extraction process.

V. CONCLUSIONS

Experimental results showed that the proposed method achieved higher embedding capacity (25% of the cover image) than Chi-Nan Lin et al's method (19 % of the cover image.).Though hiding capacity is increased there is slight difference in the PSNR values. Average PSNR value of Chi-Nan Lin is 65.90 dB where as that of proposed method is 64.22 dB. The reference matrix used (based on 4x4 numbered table) in the experiment has 20922789888000(16!) possible variances which can improve the security of the secret data. In future, the work can be done on embedding the 4x4 numbered table itself in the Stego image to achieve higher security.

REFERENCES

[1]. Chi-Nan Lin, Chin-Chen Chang, Wei-Bin Lee and Jason Lin "A Novel Data Hiding Scheme Using a Secret Reference Matrix", 2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing.

[2]. W. Hong, T.S. Chen, and C.W. Shiu, "A Minimal Euclidean Distance Searching Technique for Sudoku Steganography," Proceedings of the International Symposium on Information Science and Engineering (ISISE2008), December 2008.

[3]. C.C. Chang, Y.C. Chou, and T.D. Kieu "An Information Hiding Scheme Using Sudoku," Proceedings of the Third International Conference on Innovative Computing, Information and Control (ICICIC2008), Dalian, China, pp. June 2008.

Authors Biography:

Laxman Tawade has pursued BE degree in Electronic & Telecommunication from Pune University, India in 2011. Currently he is member of International Association of Computer Science and Information Technology (IACSIT), Academy & industry research collaboration center (AIRCC) & Affiliate member of signal processing for communication and networking technical committee. He has 1 paper in international conference and 4 papers in International Journal to his credit. He has worked as Reviewer for international journals and international conference sponsored by IEEE & also worked as program committee member of few international conferences. His research interest includes Security & Communication Network, Optical Fiber Communication and optical access networks based on WDM-PON, Biomedical signal processing.

Mahajan Rajshree is currently an Assistant professor in the Department of Electronic & Telecommunication at Aditya Engineering College, Beed, India. She is completed first part of M.E. Electronics from Govt. Engg. College, Aurangabad, MH,India. His teaching experience is 6 years. She has 2 National conference papers. His research interest includes Robot Arm control via Internet, Low power VLSI, Security&CommunicationNetwork.

Chandan Kulthe is pursuing BE degree in Electronic & Telecommunication from Dr.Babasaheb Ambedkar Marathwada University, India. His research interest includes Security & Communication Network, Optical Fiber Communication and optical access networks based on WDM-PON.