I. J. Computer Network and Information Security, **2013, 5, 40-46**
Published Online April 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2013.05.05

A Bespoke Technique for Secret Messaging

Mahimn Pandya
Smt. K.B.Parekh College of CS, Bhavnagar University
mahimn009@gmail.com

Hiren Joshi
Department of Computer Science, Gujarat University
hirenjoshirajkot@gmail.com

Ashish Jani
PDF Computer Science & Engg, Florida Atlantic University, USA
ajani@fau.edu

Abstract **—** The communication of digital assets on the internet infrastructure is increasing in its volume with threats on its security with regard to active and passive attacks of eavesdroppers. This concern has opened up the research channel to improve the techniques of secure and reliable communication protecting intellectual property rights and message security. Constant efforts of researchers in this area to achieve communication at faster rate maintaining security of digital assets, is giving improved techniques to achieve the goal. The efforts made here in this work are in the direction to enhance level of security in making faster reliable and secure communication. In spite of continued efforts, still as on today, it is challenging to hide the communication from eavesdropper. The disciplines of Cryptography, Steganography and Digital Watermarking are still popular areas of research. They are continuously digging to find robust and effective algorithms to protect digital communications and digital assets. It is very true that if the complexity in algorithm is increased, higher security level can be achieved. In the reviewed work, Researchers have developed algorithms for text encryption and embedment in digital watermarking using LSB at cost of time. The proposed work is targeted to maintain the tradeoff between the complexity level of algorithm and security level of message considering the time factor. The proposed work has evolved with two algorithms: AMEADT (ASCII Message Encryption and Decryption Technique) to protect secret message and AMEAET (ASCII Message Embedment and Extraction Technique) to embed encrypted text to digital image. The implementation of these algorithms has resulted in justifying higher level of security with comparatively lower level of complexity of algorithm.

Index Terms **—** Steganography, Hiding Information, Image Pixel Values, AMEADT, AMEAET, Cipher Text, Key

I. INTRODUCTION

Digital assets are suffering from ownership issues. Enormous efforts are put to research out more and more improve techniques for hiding secret messages in target images without increasing the size and visual texture of the image [1, 2 and 3]. Though success to certain extent has been achieved, more robust work is needed for hiding secret messages from eavesdroppers. Steganography and Cryptography in combination come for this help. The secret message which is to be communicated is in its hidden state so that it does not come to the notice of eavesdropper [4, 5 and 6]. Under the banner of cryptography the secret message is first encrypted with a key and then this encrypted message is sent to destination. The key is to be sent hiddenly. This poses two fold challenges because at the destination the encrypted message should be received and decrypted with the key. No one can decrypt without key. The adopted approach can be that the encrypted message can be embedded to target image and then embedded image is sent to destination. This gives a feel of image communication rather than of secret message communication, this falls under the banner of Steganography.

Here, there is a challenge of sending encryption key and embedment key. In case of embedment key, there are two options – static key or dynamic key. The dynamic key provides more robust secrecy compare to static key [7, 8]. Use of dynamic key is adopted in this work and to improve secrecy of message. The use of symmetric cryptography is considered with encryption and decryption using same key [9, 10 and 11].

Further, the key used in symmetric cryptography is also used in embedment of encrypted message to the digital image. This kind of work is not traced in literature survey. The single key, which is used for encryption and embedment at source and extraction and decryption at destination, serves the purpose of simplicity of algorithm. The management of key is easy but at the first sight it appears to be "the secrecy

of the key is a crucial issue". In the adopted approach, the disclosure of key does not give the decryption and extraction easily because the key is same in both the processes but the algorithms are different and not known to eavesdropper.

At destination end, the algorithm extracts the encrypted message from an image using key. Then the communicated key will be used to decrypt the secret message. After the extraction, the same key will be utilized for decryption of separate encrypted message to get the secret message in its original form. Encryption text key is decided on the basis of size of text message. The proposed algorithm does not permit repetition of character in key.

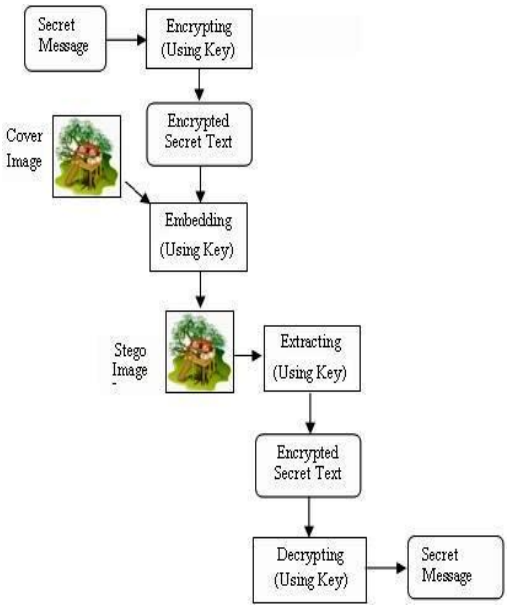

Figure 1 Secret text message embedment and extraction process proposed work

A. ASCII Concept

American Standard Code for Information Interchange (ASCII) is standardized by American National Standard Institute (ANSI) standard. It is based on A-Z, a-z and 0-9 basically [12].

This character starts with 65 for capital letters. For example for ASCII value of capital **A** is 65 and small a is 97. The code is used here for key to encrypt and embed at source and extract and decrypt at destination [13].

II. REVIEW OF RELATED WORK

The message encryption technique and message embedding technique to digital image are given by researchers. The previous technique deals with both cryptographic and watermarking algorithm. Researchers use MSA [14 and 15] as a key which is used to encrypt watermark before embedding to digital image and have used LSB technique to embed message to digital image.

Review of the work highlights complex and time consuming encryption technique. In development of cryptographic technique the researchers have focused on cryptographic and steganographic techniques [16-20].

In proposed work the focus is not only on cryptographic techniques but also tried to achieve security level high by modifying message embedment technique. The proposed work deals with embedment of cipher text (secret text) using a key which is used for encryption at one end and for decryption at another end.

III. PROPOSED WORK

Proposed algorithm, AMEADT is used to encrypt and decrypt secret message. This algorithm is based on ASCII value of a secret key. Another algorithm AMEAET is used to embed and extract secret message from digital image. This is using ASCII value to decide the position of embedment in image pixel matrix.

This technique follows the method of cryptography to encrypt and decrypt text message using ASCII value of a key. Here, key is dynamic so protection is comparatively high.

The process of encryption is as follows here we have key "MESAGT" as an experiment and all experiments have been done based on that.

A. AMEADT (ASCII Message Encryptions and Décryptions Technique)

Step 1 Find the ASCII value of Key as shown in Table I.

TABLE I KEY AND ASCII VALUE OF KEY

Key Text	ASCII value
M	77
E	69
S	83
A	65
G	71
T	84

Step 2 Sort those in ascending order as shown in Table II

TABLE II SORTED FORM OF KEY

Key Text	ASCII value
A	65
E	69
G	71
M	77
S	83
T	84

Step3 Find the ASCII value of "Original Secret Message". Here secret message is "SECRET" as shown in Table III

TABLE III SECRET TEXT AND ITS ASCII VALUE

Secret Text	ASCII Value of Secret Text
S	83
E	69
C	67
R	82
E	69
T	84

Step4 Add Sorted form of ASCII value of Key into Original Secret Message for Encryption as shown in Table IV

TABLE IV ENCRYPTED TABLE FOR GIVEN EXAMPLE

Key in Ascending order	ASCII of Key	OSM	ASCII of OSM	Encrypt Value
A	65	S	83	148
E	69	E	69	138
G	71	C	67	138
M	77	R	82	159
S	83	E	69	152
T	84	T	84	168

Encrypted value, shown in Table IV, is embedded to digital image using AMEAET. At destinations this data are extracted and decrypted by applying reverse process. The recipient will receive the stego image only an

B. AMEAET (ASCII Message Embedment and Extraction Technique)

Step1 Select the pixel value shown in Fig. 2 is according to ASCII value in ascending order.
Here code is {65, 69, 71, 77, 83, and 84}
So value is placed at {(6,5), (6,9), (7,1), (7,7), (8,3), and (8,4)}

	1	2	3	4	5	6	7	8	9
1									
2									
3									
4									
5									
6					■				■
7	■						■		
8			■	■			■		

Figure 2 Position selected according to ASCII value of Key.

Step2 Encrypted value is embedded at selected position. Select the pixel value positions shown in Fig. 2 is changed with Encrypted Value Show in Table IV as resulted shown in Fig.3.

	1	2	3	4	5	6	7	8	9
1									
2									
3									
4									
5									
6					148				138
7	138						159		
8			152	168					

Figure 3Position selected according to ASCII value of Key changed with Encrypted Value

Now this will generate stego-image having embedment of encrypted text.

For extraction of encrypted text same process of selection of position using key will be used to identify embedded text on image

IV. EXPERIMENTS AND RESULTS

The proposed algorithms are experimented in SCILAB [21] environment using various grayscale images of various sizes having resolution > 256 x 256. Here “Barbara.jpg” and “boat.jpg” images are shown.
Plain text: “SECRET “
Key: MESAGT
Encrypted Value is: {148, 138,138,159,152,168}
Embedment Position: Shown in Fig.2 (as per key)

(a)

180	200	205	192	190	193	196	206	212
175	197	201	189	190	193	196	207	214
173	195	194	183	188	193	198	210	211
183	200	193	181	187	193	200	213	212
197	208	194	184	190	194	201	212	208
199	203	190	187	194	196	204	211	202
195	193	183	188	197	199	208	211	199
195	190	180	190	199	201	211	212	186
202	192	189	195	204	207	214	208	177

(b)

Figure 4 (a) Barbara cover image of 512x512 pixels.
(b) 9x9 pixel matrix of image Fig. 4 (a)

(a)

180	200	205	192	190	193	196	206	212
175	197	201	189	190	193	196	207	214
173	195	194	183	188	193	198	210	211
183	200	193	181	187	193	200	213	212
197	208	194	184	190	194	201	212	208
199	203	190	187	148	196	204	211	138
138	193	183	188	197	199	159	211	199
195	190	152	168	199	201	211	212	186
202	192	189	195	204	207	214	208	177

(b)

Figure 5 (a) stego image of 512x512 pixels.
(b) 9x9 pixel matrix of image Fig. 5(a)

(a)

128	123	126	117	127	124	125	129	126
129	126	128	123	125	124	124	129	126
127	126	128	127	123	126	126	130	129
125	124	128	128	123	126	128	129	130
126	126	128	127	124	125	129	126	129
126	127	127	125	126	126	130	126	130
124	130	124	125	124	127	129	127	130
124	134	123	125	121	126	124	125	127
126	127	126	127	126	124	126	132	127

(b)

Figure 6 (a) boat cover image of 512x512 pixels.

(b) 9x9 pixel matrix of image Fig. 6(a)
(a)

128	123	126	117	127	124	125	129	126
129	126	128	123	125	124	124	129	126
127	126	128	127	123	126	126	130	129
125	124	128	128	123	126	128	129	130
126	126	128	127	124	125	129	126	129
126	127	127	125	148	126	130	126	138
138	130	124	125	124	127	159	127	130
124	134	152	168	121	126	124	125	127
126	127	126	127	126	124	126	132	127

(b)

Figure 7 (a) stego image of 512x512 pixels.
(b) 9x9 pixel matrix of image Fig. 7(a)

The encrypted value is embedded to an image as a result the stego images are generated. Stego images shown in Fig. 5(a) and Fig. 7(a) seem to have no change apparently. There is change but it seems in Fig. 5(b) and Fig. 7(b) but this is not visualized in stego images by naked eyes. The embed message size and key size must be less than 255 characters. This is how we can hide communication.

At the other end, authentic person having key extracts pixel value, by using key and subtract key value from that extracted values as shown in Table 5, can reveal the message.

TABLE V DECRYPTION TABLE FOR CURRENT KEY

Key in Asc. order	ASCII of Key	Stego image (x, y)	Extracted – Key	Decrypted Value	SM
A	65	(6,5)	148-65	83	S
E	69	(6,9)	138-69	69	E
G	71	(7,1)	138-71	67	C
M	77	(7,7)	159-77	82	R
S	83	(8,3)	152-83	69	E
T	84	(8,4)	168-84	84	T

V. CONCLUSION

In this paper, a technique is proposed which increases the level of secrecy in communication. This improvement in secrecy level is achieved by combining the techniques: AMEADT and AMEAET using single key for both encryption/decryption and embedment/extraction. The earlier work had a focus on improving the complexity of encryption and using static technique of embedment. This approach does take special care of the security level in the embedment phase.

The increasing complexity in any technique may increase the level of security but it will take much encryption and decryption process time. The proposed work takes special care to increase the level of secrecy in encryption by user defined dynamic key, without increasing the complexity of algorithm. This reduced complexity is achieved by using the same dynamitic key for embedment. This leads to the enhancement of secrecy level.

This research work has a limitation with regard to the size of message to be communicated has to be less than 255 characters in size. This limitation may fruitful when message is communicated in form of two or three fragments which can be integrated at end. The use of this technique will increase the level of secrecy. The proposed work using message limited to 255 characters. The message of this size has requirement of image object for embedment must have resolutions greater than 256x256 pixels. The larger the image than the message size will not change the entire image pixel. As result of this the change in image appearance will not be noticeable and reduce the apparent doubt of embedment.

ACKNOWLEDGEMENT

We are heartily thankful to Dr. N.N. Jani, Dean. Department of Computer Science, KSV, Gandhinagar, for giving thorough knowledge of SCILAB (SIP) and fatherly attention while research was being done. We are also thankful to him for cultivating research attitude in our soul.

REFERENCES

[1]. R. Amirtharajan, R. Akila, and P. Deepikachowdavarapu, *"A comparative Analysis of Image Steganography",* International Journal of computer Applications (0975-8887), May, 2010, Vol 2, No. 3.

[2]. Bret Dunber, *"Steganographic Techniques and their use in an Open-Systems Environment",* SANS Institute, 01/18/2002.

[3]. D. Aucsmith, *"An information-theoretic model for steganography",* Proceedings of the second Intel. Workshop on Information Hiding, April, 1998, pg. 306-318.

[4]. J. Nath, "Advanced Steganography Algorithm using Encrypted secret message,", IJCSA, vol. 2, no. 3, 2011.

[5]. A. Nath, S. Ghosh, M. A. Mallik, "Symmetric Key Cryptography using Random Key generator:" Proceedings of International conference on security and management(SAM2010) held at Las

Vegas, USA Jully 12-15, 2010), P-Vol-2, 239-244 (2010).

[6]. J. Nath and A. Nath, "Advanced Steganography Algorithm using encrypted secret message" International Journal of Advanced Computer Science and Applications, Vol-2, No-3, Page-19-24, March(2011).

[7]. D. Chatterjee, J. Nath, S. Dasgupta and A. Nath, "A new Symmetric key Cryptography Algorithm using extended MSA method :DJSA symmetric key algorithm", Proceedings of IEEE CSNT-2011 held at SMVDU(Jammu) 3-5 June,2011, Page-89-94.

[8]. N. Khanna, J. James, J. Nath, S. Chakraborty, A. Chakrabarti and A. Nath "New Symmetric key Cryptographic algorithm using combined bit manipulation and MSA encryption algorithm: NJJSAA symmetric key algorithm" Proceedings of IEEE CSNT-2011 held at SMVDU(Jammu) 03-06 June 2011, Page 125-130.

[9]. D. Das, J. Nath, M. Mukherjee, N. Chaudhury and A. Nath, "An Integrated symmetric key cryptography algorithm using generalized vernam cipher method and DJSA method: DJMNA symmetric key algorithm", Proceedings of IEEE conference WICT-2011 held at Mumbai University Dec 11-14,2011

[10]. J. Nath. et. al. "Symmetric key Cryptography using two-way updated -Generalized Vernam Cipher method: TTSJA algorithm" IJCA, *Volume 42– No.1, March 2012*

[11]. D. Chatterjee, J. Nath, S. Das, S. Agarwal and A. Nath, "Symmetric key Cryptography using modified DJSSA symmetric key algorithm", Proceedings of International conference Worldcomp 2011 held at Las Vegas, USA, July 18-21, Page 312-318, Vol-I(2011).

[12]. D. Chatterjee, J. Nath, S. Mondal, S.eep Da.key Cryptography using extended MSA method: DJSSA symmetric key algorithm" Jounal of Computing, Vol3, issue-2, Page 66-71,Feb(2011).

[13]. M. Sreerama Murty, D. Veeraiah, and a Srinivas Rao, "Digital Signature and Watermark Methods For Image Authentication using Cryptography Analysis," *Signal & Image Processing : An International Journal*, vol. 2, no. 2, pp. 170–179, Jun. 2011.

[14]. A. Houmansadr and S. Ghaemmaghami, "A Digital Image Watermarking Scheme Based on Visual Cryptography *," pp. 1–5.

[15]. Cryptography and Network, Willian Stallings, Prentice Hall of India.

[16]. I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*, Second Edi. Morgan Kaufmann Publishers, Elsevier, 2008.

[17]. http://www.fi.muni.cz/ Definition of Steganography [ppt CHAPTER 13 - Steganography and Watermarking]

[18]. Ismail Avcıbas¸, Member, IEEE, Nasir Memon, Member, IEEE, and Bülent Sankur, Member, IEEE, "Steganalysis Using Image Quality Metrics", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 12, NO. 2, FEBRUARY 2003

[19]. R. L. de Queiroz, "Processing JPEG-compressed images and documents.," *IEEE transactions on image processing : a publication of the IEEE Signal Processing Society*, vol. 7, no. 12, pp. 1661–72, Jan. 1998..

[20]. M. Sreerama Murty, D. Veeraiah, and a Srinivas Rao, "Digital Signature and Watermark Methods For Image Authentication using Cryptography Analysis," *Signal & Image Processing : An International Journal*, vol. 2, no. 2, pp. 170–179, Jun. 2011.

[21]. Raman, S. (2010). Image Processing Using Scilab, 1–29.

Mr. Mahimn B. Pandya is an Assistant Professor of Computer Science at Smt. K. B. Parekh College of Computer Science, Mahuva, Maharaja Krushnakumarsinhji Bhavnagar University. In teaching, he has been imparting knowledge in Operations Research, Cryptography & Network Security, and Data Structure. He is currently pursuing M. Phil. in Computer Science from KSV, Gandinagar.

Dr. Hiren Joshi is working as Assistant Professor of Computer Science at Dept. of Computer Science, Gujarat University. He has 10+ years of teaching experience. His teaching experience includes various master programs - MCA, M.Tech., PGDCSA, M.Sc [IT & CA]. He has written a book on Web Technology. His research interest includes Biometric Authentication, DBMS and Information Security.

Dr. Ashish Jani is working as Assistant Professor in MCA Department of S K Patel Institute of Management & Computer Studies. He has total teaching experience of 5 years. He is teaching in MCA Programme as well as M.Sc. (IT) program of Kadi Sarva Vishwa Vidyalaya, Gandhinagar. He has got funded project from GUJCOST. He actively

involved in consultancy work. Area of Interest: Embedded System with RTOS, C#, ASP.NET, Mobile Computing.Currently he is working on computer vision, as post doctoral research fellow at Florida Atlantic University, Boca Raton, FL, USA for the period Oct 2012 to Mar-2013.

