Volume 2, No. 4, April 2011
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

Text Steganography using Article Mapping Technique(AMT) and SSCE

Indradip Banerjee[*1], Souvik Bhattacharyya[2] and Gautam Sanyal[3]

*[1] Department of Computer Science and Engineering, University Institute of Technology
The University of Burdwan, Burdwan, India.
ibanerjee2001@yahoo.com [1]
[2] Department of Computer Science and Engineering, University Institute of Technology
The University of Burdwan, Burdwan, India.
souvik.bha@gmail.com [2]
[3] Department of Computer Science and Engineering, National Institute of Technology
Durgapur, India.
nitgsanyal@gmail.com [3]

Abstract: In this contribution we present a novel work of text steganography. Now a days, maintain the security of the secret data has been a great challenge. Sender can encrypt the message before sending it. Encrypted messages sending frequently through a communication channel like Internet, draws the attention of third parties, hackers and crackers, perhaps causing attempts to break and reveal the original messages. Steganography is a promising area which is used for secured data transmission over any public media. Considerable amount of work has been carried out by different researchers on steganography. In this paper, a steganographic model has been proposed which has more embedding capacity of text based steganography technique for communicating information more securely between two locations is proposed. The authors incorporated the idea of secret key for authentication at both ends in order to achieve high level of security. As a further improvement of security level, the information has been encoded through SSCE values and embedded into the cover text using the proposed text steganography method to form the stego text. This encoding technique has been used at both ends in order to achieve high level of security. At the receiver side different reverse operation has been carried out to get back the original information.

Keywords: Text Steganography, Article Mapping Technique (AMT), Cover Text, Stego Text, SSCE (Secret Steganography Code for Embedding).

INTRODUCTION

Now a days, the internet expand rapidly that it has become a common communication channel. In this open channel the information can be transmit secretly, so it is now becomes an important topic. The term steganography is one of the approaches to do this [13, 10]. In fact several examples from the times of ancient Greece are available in Kahn [5]. In recent years, everything is trending toward digitalization and with the rapid development of the Internet technologies, digital media can be transmitted conveniently over the network. Therefore, messages need to be transmitted secretly through the digital media by using the steganography techniques. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret [9, 25]. Another form of information hiding is digital watermarking, which is the process that embeds data called a watermark, tag or label into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. The object may be an image, audio, video or text only [12]. Although steganography is an ancient subject, the modern formulation of it comes from the prisoner's problem proposed by Simmons [1].An assumption can be made based on this model is that if both the sender and receiver share some common secret information then the corresponding steganography protocol is known as then the secret key steganography where as pure steganography means that there is none prior information shared by sender and receiver. If the public key of the receiver is known to the sender, the steganographic protocol is called public key steganography [4, 8]. Although all digital file formats can be used for steganography, but the image and audio files are more suitable because of their high degree of redundancy [25]. Fig. 1 below shows the different categories of file formats that can be used for steganography techniques now a day.

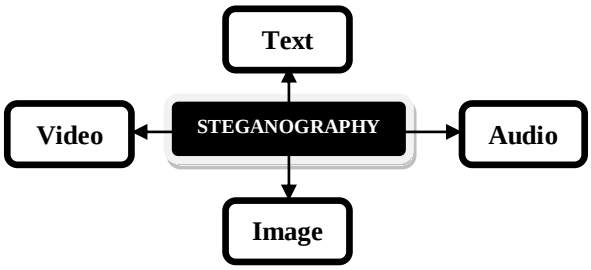

Figure 1: Types of Steganography

Among them image steganography is the popular of the lot. In this method the secret message is embedded into an image as noise to it, which is nearly impossible to differentiate by human eyes [11, 15, 17]. In video steganography, same method may be used to embed a message [18, 24]. Audio steganography embeds the message into a cover audio file as noise at a frequency out of human hearing range [19]. One major category, perhaps the most difficult kind of steganography is text steganography or linguistic steganography [3]. The text steganography is a method of using written natural language to conceal a secret message as defined by Chapman et al. [16].

A block diagram of a generic form of steganographic system is given in Fig. 2. A message is embedded in a carrier (cover carrier) through an embedding algorithm, with the help of a secret key. The resulting stego carrier is transmitted over a channel to the receiver where it is processed by the

extraction algorithm using the same key. During transmission the stego carrier, it can be monitored by unauthenticated viewers who will only notice the transmission of an image without discovering the existence of the hidden message.

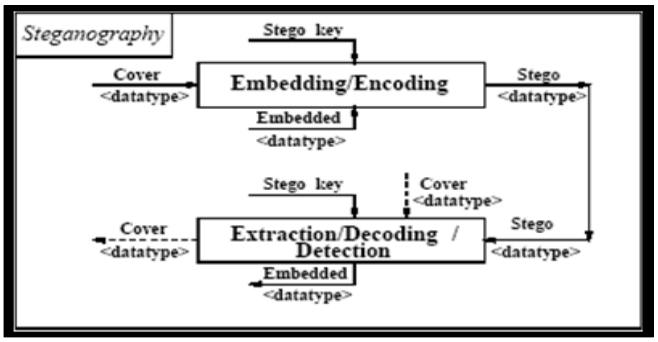

Figure 2: Generic steganographic system

This paper has been organized as following sections:- Section II discusses about some of the related works done based on text steganography steganography. Section III describes the SSCE method for text message encryption. Section IV describes proposed text steganography method (AMT). Section V and VI deals with proposed data hiding model and the solution methodology, Section VII describes different algorithms for different processes used at both at sender side and receiver side. Section VIII discusses the computer algorithm. Experimental results are shown in Section XI. Section X contains the analysis of the results and Section XI draws the conclusion.

RELATED WORKS ON TEXT STEGANOGRAPHY

Text steganography can be broadly divided into three types. They are format-based, random & statistical generations and Linguistic method shows in Figure 3. Most peoples have suggested various methods for hiding information in text in mentioned three categories. Some of the methods are discussed in this paper. Format-based methods use and change the formatting of the cover-text to hide the data. They don't change any words or sentences, so it does not harm the 'value' of the cover-text. A format-based text steganography method is open space method. In this method extra white spaces are added into the text to hide information. These white spaces can be added after end of each word, sentence or paragraph. A single space is interpreted as "0" and two consecutive spaces are interpreted as "1" [6]. Although a little amount of data can

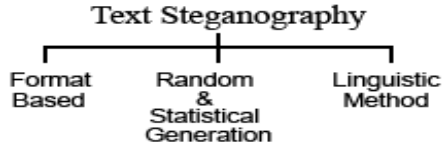

Figure 3: Three broad categories of text steganography

be hidden in a document, this method can be applied to almost all kinds of text without revealing the existence of the hidden data. Another two format-based methods are word shifting and line shifting. In word shifting method, the horizontal alignments of some words are shifted by changing distances between words to embed information [21]. These changes are hard to interpret because varying distances between words are very common in documents. Another method of hiding information is, in manipulation of whitespaces between words and paragraph [27]. In line shifting method, vertical alignments of some lines of the text are shifted to create a unique hidden shape to embed a message in it [23]. Random and statistical generation methods are used to generate cover-text automatically according to the statistical properties of language. These methods use example grammars to produce cover-text in a certain natural language. A probabilistic context-free grammar (PCFG) is a commonly used language model where each transformation rule of a context-free grammar has a probability associated with it [2]. A PCFG can be used to generate word sequences by starting with the root node and recursively applying randomly chosen rules. The sentences are constructed according to the secret message to be hidden in it. The quality of the generated stego-message depends directly on the quality of the grammars used. Another approach to this type of method is to generate words having same statistical properties like word length and letter frequency of a word in the original message. The words generated are often without of any lexical value. The last category, the linguistic method considers the linguistic properties of the text to modify it. The method uses linguistic structure of the message as a place to hide information. Syntactic method is a linguistic steganography method where some punctuation signs like comma (,) and full-stop (.) are placed in proper places in the document to embed a data. This method needs proper identification of places where the signs can be inserted. Another linguistic steganography method is semantic method. In this method the synonym of words for some pre-selected are used. The words are replaced by their synonyms to hide information in it [20]. Except the above mentioned methods, there are some other methods for text steganography, such as feature coding, text steganography by specific characters in words, abbreviations etc. [26] or by changing words spelling [28].

In this paper, a secret key steganographic model for text based steganography technique for communicating information more securely between two locations has been proposed which first uses a plain text as the cover data and the secret message is embedded in the cover data to form the stego text. The AMT text steganography scheme has been inspired by the author's previous work [29, 30, 32, 33, 34, 35]. In paper [29, 30], by indefinite articles '*a'* or '*an'* in conjunction with the non-specific or non-particular nouns in English language based on the mapping information according to the embedding sequence has been introduced. Here data embedding in various characters which are selected by the system dynamically with the help of cover text. The embedding capacity is also increased due to set of articles or characters are used for mapping technique. The author incorporated the idea of encoding through SSCE values before embedding to achieve high level of security. This work proposes a new algorithm with higher security features so that the embedded message can not be hacked by unauthorized user.

METHOD FOR DATA ENCODING (SSCE)

The input messages can be in any digital form and are often treated as a bit stream. The input message is first encrypted using a code generation technique SSCE [29, 35]. For the improvement of security level, the SSCE code representation has been used to encrypt the message and

then secret message has been embed to the cover text.

Secret Steganography Code for Embedding(SSCE) Table

ASCII	SSCE	ASCII	SSCE	ASCII	SSCE	ASCII	SSCE	ASCII	SSCE	ASCII	SSCE	ASCII	SSCE	ASCII	SSCE	ASCII	SSCE	ASCII	SSCE
10	1	1	26	2	52	3	78	4	104	5	130	6	156	7	181	8	206	9	231
20	2	11	27	12	53	13	79	14	105	15	131	16	157	17	182	18	207	19	232
30	3	21	28	22	54	23	80	24	106	25	132	26	158	27	183	28	208	29	233
40	4	31	29	32	55	33	81	34	107	35	133	36	159	37	184	38	209	39	234
50	5	41	30	42	56	43	82	44	108	45	134	46	160	47	185	48	210	49	235
60	6	51	31	52	57	53	83	54	109	55	135	56	161	57	186	58	211	59	236
70	7	61	32	62	58	63	84	64	110	65	136	66	162	67	187	68	212	69	237
80	8	71	33	72	59	73	85	74	111	75	137	76	163	77	188	78	213	79	238
90	9	81	34	82	60	83	86	84	112	85	138	86	164	87	189	88	214	89	239
100	10	91	35	92	61	93	87	94	113	95	139	96	165	97	190	98	215	99	240
110	11	101	36	102	62	103	88	104	114	105	140	106	166	107	191	108	216	109	241
120	12	111	37	112	63	113	89	114	115	115	141	116	167	117	192	118	217	119	242
130	13	121	38	122	64	123	90	124	116	125	142	126	168	127	193	128	218	129	243
140	14	131	39	132	65	133	91	134	117	135	143	136	169	137	194	138	219	139	244
150	15	141	40	142	66	143	92	144	118	145	144	146	170	147	195	148	220	149	245
160	16	151	41	152	67	153	93	154	119	155	145	156	171	157	196	158	221	159	246
170	17	161	42	162	68	163	94	164	120	165	146	166	172	167	197	168	222	169	247
180	18	171	43	172	69	173	95	174	121	175	147	176	173	177	198	178	223	179	248
190	19	181	44	182	70	183	96	184	122	185	148	186	174	187	199	188	224	189	249
200	20	191	45	192	71	193	97	194	123	195	149	196	175	197	200	198	225	199	250
210	21	201	46	202	72	203	98	204	124	205	150	206	176	207	201	208	226	209	251
220	22	211	47	212	73	213	99	214	125	215	151	216	177	217	202	218	227	219	252
230	23	221	48	222	74	223	100	224	126	225	152	226	178	227	203	228	228	229	253
240	24	231	49	232	75	233	101	234	127	235	153	236	179	237	204	238	229	239	254
250	25	241	50	242	76	243	102	244	128	245	154	246	180	247	205	248	230	249	255
		251	51	252	77	253	103	254	129	255	155								

Figure 4: SSCE Value Table

AMT METHOD FOR TEXT STEGANOGRAPHY

The proposed secret-key text steganographic model has been discussed in previous work [29]. The input messages can be in any digital form and are often treated as a bit stream. The input message is first encrypted and generates the secret key, (which may be called a message enabled key). Before embedding a checking has been done to find out whether the double letter word in the given cover text (e.g. "food" – 'o' is double here), if not assume the first letter. Then system will search out the corresponding group of letters which are mapped with that double letter (e.g. here 'o'). Secret message has been embed to the cover text by inserting that particular group of letters based on the mapping information shown in Fig 5 to form the stego text. At the receiver side other different reverse operation has been carried out to get back the original information.

a	00	01	10	11
	b	c	d	e
	f	g	h	i
	j	k	l	m
	n	o	p	q
	r	s	t	u
	v	w	x	y
	z			

b	00	01	10	11
	c	d	e	f
	g	h	i	j
	k	l	m	n
	o	p	q	r
	s	t	u	v
	w	x	y	z
	a			

c	00	01	10	11
	d	e	f	g
	h	i	j	k
	l	m	n	o
	p	q	r	s
	t	u	v	w
	x	y	z	a
	b			

z	00	01	10	11
	a	b	c	d
	e	f	g	h
	i	j	k	l
	m	n	o	p
	q	r	s	t
	u	v	w	x
	y			

Figure 5: Mapping Technique

THE AMT MODEL

Fig. 6 shows the block diagram of the AMT secret-key steganographic model. This input message is first converted into encrypted form using SSCE values. This encrypted message generates the secret key. The encrypted message then embedded in the cover text using the mapping technique method shown in Fig 6 to form the stego text and

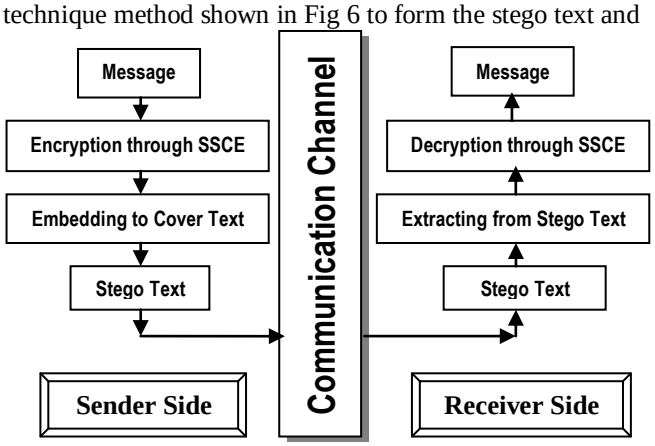

Figure 6: AMT Steganography Model

transmit to the receiver side. At the receiver side, the extraction process starts by extracting the encrypted message from the stego text. Next the stego text goes through the text decryption method and finally the receiver may be able to see the embedded message with the help of same secret key generated at the sender side.

SOLUTION METHODOLOGY

The AMT system consists of following two windows, one at the SENDER SIDE and the other at the RECEIVER SIDE.

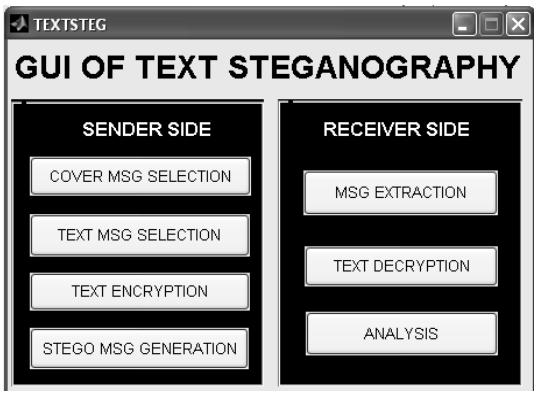

Figure 7: GUI based steganography system

The user will be someone who is familiar with the process of information hiding and will have the knowledge of steganography systems. An encryption algorithm has been proposed prior to steganography for generation of encoded message. The user should be able to select a plain text message from a file, another text to be used as the carrier (cover text) and then use the proposed embedding method which will hide the encrypted message in the selected cover text and will form the stego text. The user at the receiver side should be able to extract the message from the stego text with the help of different reverse process in sequential manner to un-hide the message from the stego text. The GUI of the proposed solution has been shown in figure 7.

ALGORITHMS

In this section, algorithms for different processes of text and image based steganography used both in the sender side and receiver side are discussed. Fig.8 shows the algorithm of proposed (AMT) system.

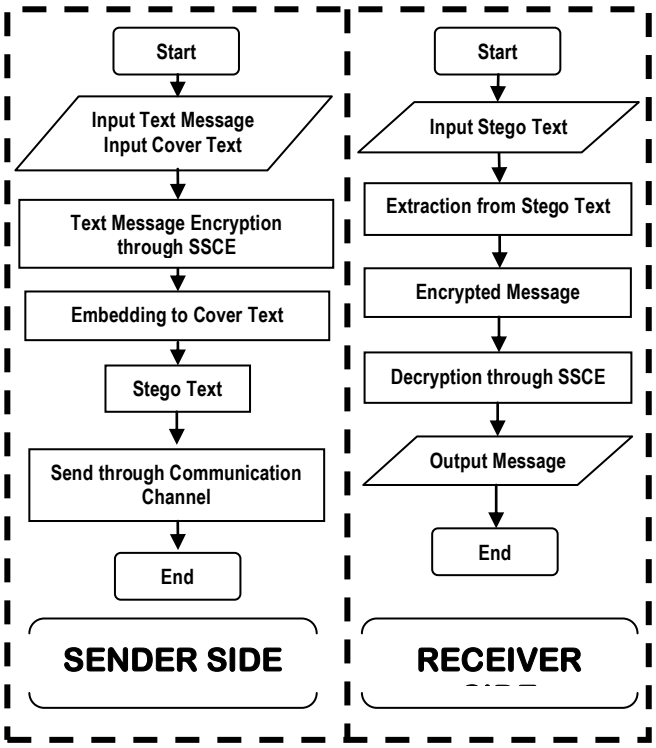

Figure 8: AMT Algorithm for Steganographic Model

A. *Algorithm for Message Encryption / Decryption*

- Select the message and pick one by one character.
- Convert to its ASCII equivalent.
- Change ASCII code to our generated code from *SSCE* Table (Figure 4).
- Convert to its character equivalent.

B. *Algorithm for Message Embedding for Stego Text formation*

- Select the message and find out the double letter word in the cover text, if not assume the first letter.
- Search out the corresponding group of letters which are mapped with that double letter.
- Encrypt the message with *SSCE value*.
- Select the cover text to embed the message. Check whether the selected text is capable of embedding. If not possible repeat this step otherwise continue.
- Check the message sequence and pick first two bit sequence (MSG).
- Starting from the first word of the cover text (TX)
  - If MSG=’11’ then find out the letter of group 11 and store the position in an array.
  - Else If MSG=’10’ then find out the letter of group 10 and store the position in an array.
  - Else If MSG=’01’ then find out the letter of group 01 and store the position in an array.
  - Else If MSG=’00’ then find out the letter of group 00 and store the position in an array.
- Repeat the above step for the remaining bit sequence of the message (two bit at a time).
- Save the embedding position in a separate file and encode it with *SSCE value* and send it to the receiver separately.

C. *Algorithm for Message Extractingfrom the Stego Text*

- Select the generated text (stego text) after message embedding and their positions.
- Find out the double letter word in the stego text, if not assume the first letter.
- Select the embedding position and stego text
  - If letter of group 11, then MSG=’11’
  - Else If letter of group 10, then MSG=’10’
  - Else If letter of group 01, then MSG=’01’
  - Else If letter of group 00, then MSG=’00’
- Decode the MSG with the help of *SSCE Value*.

COMPUTER ALGORITHM

In this section the two algorithimic approach is discussed one for the function of the Sender Side and another for the Receiver Side.

A. *Sender side*

- Select the Cover Text from the set of text files.
- Select the Secret message in text form.
- Encrypt the message through *SSCE Value* and also generate the Secret key.
- Embed the encrypted form of message in to the Cover text to form the Stego text.
- Transmit to communicational channel.

B. *Receiver side*

- Extract the encrypted form of secret message from the Stego text.
- Decrypt the message with the help of the previous mentioned *SSCE values* / Secret key.

EXPERIMENTAL RESULTS

This section presents the obtained results via different processes mentioned in the proposed model. The authors simulated the proposed system and the results are shown in the following figures. Fig 9, 10, 11 and 12 shows the Cover Text, Secret Message to be embedded, Encrypted Message and Stego Text respectively.

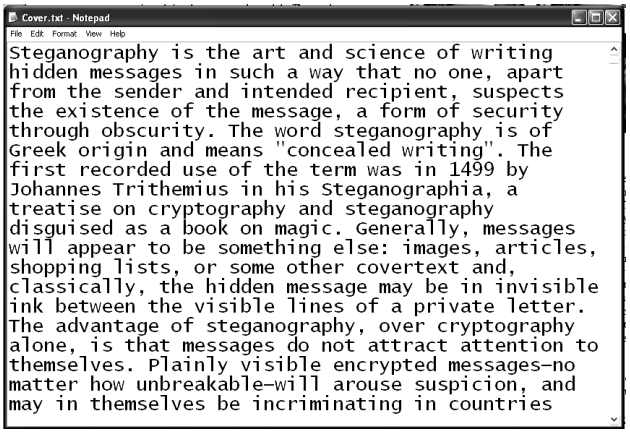

Figure 9: Cover Text

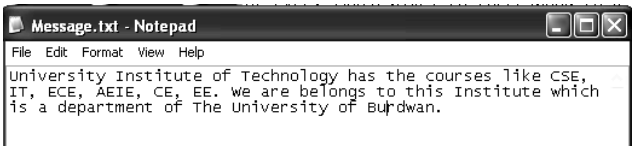

Figure 10: Message to be embedded

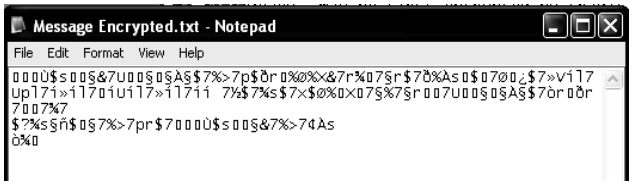

Figure 11: Encrypted Message to be embedded

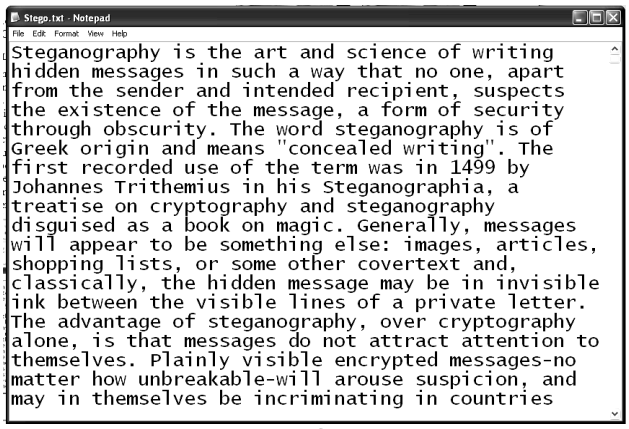

Figure 12: Stego Text

ANALYSIS OF THE RESULTS

In the previous work made by different researchers it has been seen some of the works has been done on text steganography. This work proposes a novel algorithm with higher security features of text based steganographic methods to prevent the embedded message from unauthorized user. In this work an attempt has been made to increase the level of security of the steganography model by incorporating the idea of secret key along with the use of encoded form of the original message.

The Levels of Security incorporated in the proposed model:

- Generation of the encrypted form of the secret message.
- Embedding encrypted form of the message in cover text to form the stego text using a new proposed method.
- Use of the secret key.
- All the processes both in sender side and receiver side need to be executed in proper sequence.

Similarity Measure of the Cover Text and Stego Text

Jaro-Winkler

For comparing the similarity between cover text and the stego text, the Jaro-Winkler distance for measuring similarity between two strings has been computed. The Jaro-Winkler distance [14, 7] is a measure of similarity between two strings. It is a variant of the Jaro distance metric [22], [31] and mainly used in the area of record linkage [5] (duplicate detection). The higher the Jaro-Winkler distance for two strings is, the more similar the strings are. The score is normalized such that 0 equates to no similarity and 1 is an exact match. The Jaro distance metric states that given two strings s_1 and s_2 their distance d_j is $d_j = \frac{1}{3}\left[\frac{m}{|s_1|} + \frac{m}{|s_2|} + \frac{m-t}{m}\right]$, where m is the number of matching characters and t is the number of transpositions. Two characters from s_1 and s_2 respectively are considered matching only if they are not farther than $\left\lfloor \frac{\max(|s_1|,|s_2|)}{2} \right\rfloor - 1$. Each character of s_1 is compared with all its matching characters in s_2. The number of matching (but different sequence order) characters divided by two defines the number of transpositions. The Jaro score of comparing cover text and stego text is 0.9022, which means they are closely similar. Besides comparison through histogram technique has been done. It has been observed that the histogram of the cover text and the stego text is almost identical.

Size of Cover Text	Size of Message	Jaro-Winkler	Correlation
1000	100	0.9973	6.6114e+004
1000	200	0.9973	1.3707e+005
1000	400	0.9973	2.9720e+005
1000	600	0.9973	2.7627e+005
1000	800	0.9973	7.3763e+005
2000	100	0.9987	6.4995e+004
2000	200	0.9987	1.3223e+005
4000	100	0.9993	6.4457e+004
4000	200	0.9993	1.2999e+005

Figure 13: Analysis with the help of Jaro and Correlation

In Fig 13 we observe that the Jaro-Winkler distance for measuring similarity between cover and stego has been computed. From this table it can be concluded that cover text and stego text generated after mapping of various size of secret message is almost identical. This property can be used to avoid steganalysis also.

CONCLUDING REMARKS

In this paper authors have used the new approach of text steganography to obtain secure stego-text. The SSCE code used for encrypted form of the secret message in order to achieve maximum payload and increase the security level respectively. The encrypted form of the message is embedded into the cover text to form the stego text. Here also the embedding capacity is increased, because the set of articles or characters are used for mapping technique where as the previous works done with the help of maximum three or four characters. An exactly reverse procedure is followed at the receiver side to retrieve the embedded message. The integrated approach of SSCE and a new method of text steganography have enabled the secure transfer of the message compared to earlier techniques. However to increase the security level different parameter has been considered for achieving better performance. In our next work steganalysis has also been taken care to build a commercial model.

REFERENCES

[1] Gustavus J. Simmons, "The Prisoners' Problem and the Subliminal Channel", in Proceedings of CRYPTO '83, pp 51-67. Plenum Press (1984).

[2] P. Wayner, "*Strong Theoretical Steganography*", Cryptologia, XIX(3), July 1995, pp. 285-299.

[3] J.T. Brassil, S. Low, N.F. Maxemchuk, and L. O'Gorman, "Electronic Marking and Identification Techniques to Discourage Document Copying", *IEEE Journal on Selected Areas in Communications*, vol. 13, Issue. 8, October 1995, pp. 1495-1504.

[4] "Stretching the Limits of Steganography", RJ Anderson, in Information Hiding, Springer Lecture Notes in Computer Science v 1174 (1996) pp 39-48.

[5] Kahn, The Codebreakers - the comprehensive history of secret communication from ancient times to the Internet, Scribner, New York (1996).

[6] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding", *IBM Systems Journal*, vol. 35, Issues 3&4, 1996, pp. 313-336.

[7] M. A. Jaro. Advances in record linking methodology as applied to the 1985 census of tampa florida. Journal of the American Statistical Society., 84:414–420, 1989.

[8] Scott Craver, "On Public-key Steganography in the Presence of an Active Warden," in Proceedings of 2nd International Workshop on Information Hiding, April 1998, Portland, Oregon, USA. pp. 355 - 368.

[9] Ross J. Anderson and Fabien A.P. Petitcolas, "On the limits of steganography," IEEE Journal on Selected Areas in Communications (J-SAC), Special Issue on Copyright & Privacy Protection, vol. 16 no. 4, pp 474-481, May 1998.

[10] N. F. Johnson and S. Jajodia, "Steganography: seeing the unseen," IEEE Computer.,Feb., 26-34 (1998).

[11] L. M. Marvel, C. G. Boncelet, Jr. and C. T. Retter, "Spread spectrum image steganography," IEEE Trans. on Image Processing, 8(8), 1075-1083 (1999).

[12] Digital Watermarking :A Tutorial Review S.P.Mohanty ,1999.

[13] Artz, D.: Digital Steganographic: Hiding Data within Data, IEEE Internet Comput., Vol. 5. (2001) 75-80.

[14] S. Dowdy and S. Wearden. Statistics for research. Wiley. ISBN 0471086029, page 230, 1983.

[15] Analysis of LSB Based Image Steganography Techniques ,R. Chandramouli, Nasir Memon, Proc. IEEE ICIP, 2001.

[16] M.Chapman, G. Davida, and M. Rennhard, "A Practical and Effective Approach to Large-Scale Automated Linguistic Steganography", *Proceedings of the Information Security Conference*, October 2001, pp. 156-165.

[17] An Evaluation of Image Based Steganography Methods,Kevin Curran, Kran Bailey, International Journal of Digital Evidence,Fall 2003.

[18] G. Doërr and J.L. Dugelay, "A Guide Tour of Video Watermarking", *Signal Processing: Image Communication*, vol. 18, Issue 4, 2003, pp. 263-282.

[19] K. Gopalan, "Audio steganography using bit modification", *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, (ICASSP '03)*, vol. 2, 6-10 April 2003, pp. 421-424.

[20] M. Niimi, S. Minewaki, H. Noda, and E.Kawaguchi, "A Framework of Text-based Steganography Using SD-Form Semantics Model", *Pacific Rim Workshop on Digital Steganography 2003*, Kyushu Institute of Technology, Kitakyushu, Japan, July 3-4, 2003.

[21] Y. Kim, K. Moon, and I. Oh, "A Text Watermarking Algorithm based on Word Classification and Inter-word Space Statistics", *Proceedings of the Seventh International Conference on Document Analysis and Recognition (ICDAR'03),* 2003, pp. 775–779.

[22] M. A. Jaro. Probabilistic linkage of large public health data file. Statistics in Medicine 14 (5-7), pages 491–498, 1995.

[23] A.M. Alattar and O.M. Alattar, "Watermarking electronic text documents containing justified paragraphs and irregular line spacing ", *Proceedings of SPIE - Volume5306, Security, Steganography, and Watermarking of Multimedia Contents VI*, June 2004, pp- 685-695.

[24] G. Doërr and J.L. Dugelay, "Security Pitfalls of Frameby-Frame Approaches to Video Watermarking", *IEEE Transactions on Signal Processing*, Supplement on Secure Media, vol. 52, Issue 10, 2004, pp. 2955-2964.

[25] T Mrkel,JHP Eloff and MS Olivier ."An Overview of Image Steganography,"in proceedings of the fifth annual Information Security South Africa Conference ,2005

[26] M.H. Shirali-Shahreza and M. Shirali-Shahreza, "Text Steganography in Chat", *Proceedings of the Third IEEE/IFIP International Conference in Central Asia on Internet the Next Generation of Mobile, Wireless and Optical Communications Networks (ICI 2007)*, Tashkent, Uzbekistan, September 26-28, 2007.

[27] L.Y. Por and B. Delina, "Information Hiding: A New Approach in Text Steganography", *7th WSEAS International Conference on Applied Computer & Applied Computational Science*, April 2008, pp- 689-695.

[28] MohammadShirali-Shahreza: "Text Steganography by Changing Words Spelling" at ICACT 2008.

[29] Indradip Banerjee, Souvik Bhattacharyya and Gautam Sanyal : "Novel text steganography through special code generation" at the proceedings of International Conference on Systemics, Cybernetics and Informatics (ICSCI-2011), Hyderabad, India in January 5-8, 2011.

[30] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal : "Design and implementation of a secure text based steganography model" at the Proceedings of 9th annual Conference on Security and Management (SAM) under The 2010 World Congress in Computer Science,Computer

Engineering and Applied Computing(WorldComp 2010), LasVegas,USA, July 12-15,2010.

[31] W. E. Winkler. The state of record linkage and current research problems. Statistics of Income Division, Internal Revenue Service Publication R99/04., 1999.

[32] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal : "Implementation of a Novel Text Based Steganography Model" Proceeding of "National Conference on Computing and Systems (NACCS)", 29/01/2010, Dept. of Computer Science, The University of Burdwan.

[33] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal : "A Novel Approach of Secure Text Based Steganography Model using Word Mapping Method(WMM)" Journal on "International Journal of Computer and Information Engineering 4:2 2010" - World Academy of Science, Engineering and Technology (WASET), Volume 4, Number 2, Spring 2010, Pages 96–103.

[34] Souvik Bhattacharyya, Arka Prokash Mazumdar, Indradip Banerjee and Gautam Sanyal : "Text Steganography using Formatting Character Spacing" Journal on "IJICS Vol No - 13, No. 2, Decembar, 2010".

[35] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal : "Data Hiding Through Multi Level Steganography and SSCE" Journal on "Journal of Global Research in Computer Science, Volume 2, No. 2, February 2011".

ABOUT THE AUTHORS

Indradip Banerjee received his MCA degree from IGNOU in 2009, PGDCA from IGNOU in 2008, MMM from Annamalai University in 2005 and BCA (Hons.) from The University of Burdwan in 2003. Currently he is working as a Technical Assistant in Computer Science and Engineering Department at University Institute of Technology, The University of Burdwan. His areas of interest are Network Security and Image Processing.

Souvik Bhattacharyya received his B.E. degree in Computer Science and Technology from B.E. College, Shibpur, India, presently known as Bengal Engineering and Science University (BESU) and M.Tech degree in Computer Science and Engineering from National Institute of Technology, Durgapur, India. Currently he is working as an Assistant Professor in Computer Science and Engineering Department at University Institute of Technology, The University of Burdwan. He has a good no of research publication in his credit. His areas of interest are Natural Language Processing, Network Security and Image Processing.

Gautam Sanyal has received his B.E and M.Tech degree National Institute of Technology (NIT), Durgapur, India. He has received Ph.D (Engg.) from Jadavpur University, Kolkata, India, in the area of Robot Vision. He possesses an experience of more than 25 years in the field of teaching and research. He has published nearly 50 papers in International and National Journals / Conferences. Two Ph.Ds (Engg) have already been awarded under his guidance. At present he is guiding six Ph.Ds scholars in the field of Steganography, Cellular Network, High Performance Computing and Computer Vision. He has guided over 10 PG and 100 UG thesis. His research interests include Natural Language Processing, Stochastic modeling of network traffic, High Performance Computing, Computer Vision. He is presently working as a Professor in the department of Computer Science and Engineering and also holding the post of Dean (Students' Welfare) at National Institute of Technology, Durgapur, India.