An Analysis of Alphabet-based Techniques in Text Steganography

Baharudin Osman, Azman Yasin, Mohd Nizam Omar
School of Computing, Universiti Utara Malaysia, Malaysia.
bahaosman@uum.edu.my

***Abstract*—Steganography and cryptography are methods in information hiding. Cryptography scrambles the secret message, whereas steganography conceals a secret message in a carrier medium. An audio, video, image, and text can be used as a cover medium for hiding messages in steganography. The final output of steganography is a stego object that is sent to a receiver using a stego key. Suspiciousness of a generated stego text will encourage eavesdroppers to reveal the hidden message from stego text. Having reviewed substitution, injection, and propagation techniques for steganography, this paper discovers that there is a suspicion in the generated stego text. It is also discovered that text steganography using Genetic Algorithm (GA) is less focused by researchers compared to image and audio. Accordingly, this paper proposes that the adoption of GA should be focused in future works to protect stego text from suspiciousness due to the effectiveness and efficiency used in other media. Suspiciousness against stego text is very important in steganography to avoid third parties detecting the existence of secret message.**

***Index Terms*—Cryptography; Genetic Algorithm; Mapping Method; Steganography; Suspicious Stego Text.**

I. INTRODUCTION

Information security is a big issue in recent communication field that should be considered while exchanging data in an open network. In an open network, information access is not restricted by any geographical boundary; anybody can access the data from any part of the world. Hence, transferring information via the Internet widely exposes the data to unauthorized users. To minimize security risk, information hiding methods are famously used in various areas such as military, intelligence agencies, online elections, internet banking, and medical-imaging [1].

In such context, cryptography and steganography play very important roles in protecting data during communication between two parties. Cryptography refers to the art of secret writing, in which it scrambles a secret message to avoid it from being detected by eavesdroppers. Meanwhile, steganography is the art of embedding information in a various cover objects such as audio, image, text, and video so that the eavesdroppers do not realize the presence of the secret message[2].

The word steganography origins from Greek words *steganos* (concealed or protected) and *graphein* (writing). Steganography has been around for hundreds of years and its main purpose is to pass information in a way that the third party is unaware of the presence of the secret message. One of the first recorded uses of steganography was related by the Greek historian Herodotus. It is different that cryptography, as detailed in Table 1.

Table 1
Differences between steganography and cryptography

Cryptography	Steganography
The encrypted letter could be seen by anyone but cryptography makes the message not understandable.	Steganography hides messages in another medium so that nobody notices the message.
The end result is cipher text.	The end result is stego media.
The goal is to prevent an interceptor from gaining any information about plaintext from the intercepted cipher text.	The goal is to prevent an observant intermediary from even obtaining knowledge of the mere presence of the secret data.
Any person has the ability of detecting and modifying the encrypted message.	The hidden message is imperceptible to anyone.
Steganography cannot be used to adapt the robustness of cryptographic system.	Steganography can be used together with cryptography by hiding an encrypted message.

Algorithms such as AES, DES, RSA, and hash algorithm have been used for encrypting and decrypting the secret messages in cryptography. However, the encryption algorithms can be applied in steganography methods before embedding a secret message into the cover object. The main goal of steganography is to communicate securely in a completely undetectable manner [3], and to avoid suspiciousness during data transmission.

The interest of steganography by researchers has grown in recent years [4] for two main reasons [5]. Firstly, the publishing and broadcasting industries have become interested in information hiding techniques for hiding encrypted copyright marks and serial numbers in digital films, audio recordings, books and multimedia products. Secondly, various governments have restricted the availability of encryption services, which motivate people to study methods by which private messages can be embedded in seemingly innocuous cover messages. Accordingly, [1] believes that steganography needs to be further studied to enrich the information hiding domain. Currently, most studies focus on hidden messages in image, audio, and video only, leaving text unattended.

Literatures show that three metrics have been used to measure the performance of the steganography, which are capacity, robustness, and undetectibility/imperceptibility [6][7][8][9]. Capacity refers to the amount of information that is able to be hidden in the cover medium, whereas robustness refers to the resistance of the steganography technique against

modifying or destroying the stego medium. Meanwhile, undetectibility is related to the ability of eavesdroppers to extract the hidden information easily or the difficulty of detecting the hidden information.

II. LITERATURE WORKS

Steganography can be used together with cryptography by hiding the encrypted messages in the cover text, which is known as dual steganography [1]. This adoption technique has been used in several studies [10][11]. They obtained good results when encrypted the hidden message before the hiding process. A general process of steganography involves four steps as seen in Figure 1 [12].

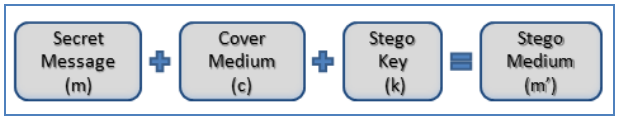

Figure 1: A general process of Steganography

where:
m : *message to be hidden*
c : *cover medium*
k : *stego key (optional)*
m' : *stego object*

In Figure 1, stego object, *m'* is the output of the steganography process that contains an embedded secret message. A medium such as audio, video, image, and text can be used as the cover medium. Protocol is another medium used by [13] for hiding information in steganography. A generated stego object should be similar with the original cover medium to disable third parties from detecting the hidden message. Embedding hidden messages along the process in Figure 1 could be done using substitution, injection, and propagation techniques.

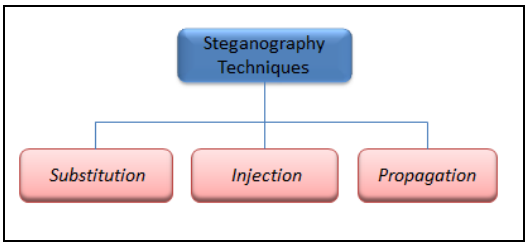

Figure 2: Steganography Techniques

In Figure 2, substitution is a technique for replacing an appropriate word or symbol or syntax of the cover text. A synonym technique is a part of linguistic steganography, which attract numerous attention of researchers now days. However, the repeating of using the same piece of text raised suspiciousness against eavesdroppers. Besides, this technique also requires a large size of a synonym dictionary to store the synonym words. Syntactic is another substitution technique that replaces the physical formatting of the text to hide a message, such as using miss spelling technique as shown in the following example:

"This is a hidden message"
"This iz a hidden message"

In the above example, the second sentence has been deliberately misspelled to hide the hidden message. The presence of error in selected word is use to transmit bit 1 and otherwise bit 0. It is very important to choose a good substitution technique to avoid a generated stego text to be suspicious. Although the substitution technique is not quite suitable in text medium because the changes in the cover text will raise suspiciousness, but is is widely used in images, audio, and video because the changes of the hidden bits does not affect the quality of stego object.

Injection technique adds something into the cover text, such as adding a space between words or at the end of the line, increases line spacing or paragraph spacing. UniSpaceCh [14] is one of the techniques. It uses a different Unicode white space character to represent the hidden message. Injection technique results in an increased file size for the stego text and raises the possibility of the suspiciousness. Although [15] claims that their proposed technique remains the stego text and the cover text similar, the stego text file increased 11.1% from the original file. The difference in the file size could lead to suspiciousness.

Lastly, propagation is a technique that does not totally depend on the cover object, but it depends on the generation engine. This technique will generate a mimic stego text based on some statistical values of the cover text such as frequency, mean, and variance. Spamimic is one example of this technique, which produces a spam file to hide a secret message. However, a communication like a spam is not allowed in most organizations and will be blocked by the network administration. Propagation technique requires high knowledge to generate correct grammar. Regarding this, researchers normally use Probabilistic Contact Free Grammar (PCFG) or Huffman code to generate new words or sentences.

Hiding a secret message in plain text can be done in many different ways, such as using white space, word or line shifting, feature encoding, syntax, and semantics methods [16]. However, they are limited in certain aspects. As an example, manipulating white space has a limitation of capacity and robustness. Whitesteg has a limited capacity to hide a large secret message and is not able to hide a high volume of message [14]. Another limitation of space manipulation is the increasing suspicion of stego text due to the ability to detect by human visual and steganalysis tool. In fact, [17] [18] discovered that space manipulation is not effective because steganalysis is able to detect 100% of the hidden message.

Semantic and syntactic are two techniques in linguistic method. Technically, syntactic places some punctuation signs in the sentence such as a comma (,) and a full stop (.). The amount for hiding information using this technique is limited (308-mandal). In semantic method, a list of synonyms of the word stored in a dictionary is used to replace a certain word in the cover text. This method produces a better quality of stego text compared to syntactic technique, but finding the hiding and replacement is a critical part and requires a high

knowledge in language grammar. However this technique is not effective for a high volume of secret message [19] and can 100% be detected by steganalysis [20][21]. Changing the spelling using American and British spelling is another technique, as visualized in Table 1. However, it has a limited capacity due to the limited the relevant words.

Table 1
American vs British Words

American Spelling	British Spelling
Airplane	Aeroplane
Color	Colour
Center	Centre
Check	Cheque
Criticize	Criticise
Favorite	Favourite
Fulfill	Fulfil

Robustness, capacity, and imperceptibility are three parameters used to evaluate the steganography performance. However, the efficiency of an algorithm is another parameter to measure the steganography performance in terms of time and memory [22].

Hiding information using alphabet (word) manipulation is more robust compare to white space approach because the hidden bit using white space is lost when the file is opened using any text editor or after performing compression or OCR tools. Therefore, most researchers use alphabet approaches such as CALP, QUARD, VERT, Symmetric and Reflection (SnR), CASE, Intelligent approach, and Nonlinear Character Position (NCP). CALP, QUAD, and Symmetric Reflection techniques are able to hide 2 bits in one character, while CASE can hide 3 bits in a single alphabet. Meanwhile, NCP and Intelligent can hide 4 bits in a single alphabet. All these techniques group the alphabets based on the characteristic of the alphabets as detailed in Table 2.

Table 2
Number of hidden bits in different techniques

	Techniques	Number of hidden bits per character
CALP ver 1 [23]	Based on the texture/pattern changes	1
CALP ver 2 [23][24]	Based on the texture/pattern changes (improvement)	2
QUARD [25] [26]	Based on the letter features which have round shapes or curve, horizontal line in the middle or diagonal line and more than one straight line	2
VERT [26]	Based on alphabets which have a vertical line	1
CASE [27]	Based on capital alphabet shape	3
SnR[28]	Based on the symmetric and reflection of alphabets	2
Unicode Character [15]	Based on the Unicode value	2
Font Type in MS Word[29]	Based on font style	Need 3 characters to hide 8 bits
Nonlinear Character Position (NCP) [30]	Based on the style of the alphabets (Bold, Italic, Underline, Arial)	4
Intelligent Approach [31]	Based on RGB color of the alphabets	4

Increasing the number of bits that can be hidden in one byte will increase the capacity of the embedded message. [30] found that NCP technique reflects the high embedding capacity of the hidden message. Instead of low capacity, [15] found that using white space and shifting techniques are not robust to OCR recognition because the hidden message is destroyed after performing the OCR tools and the steganalysis tools can extract 100% of the hidden message.

Embedding secret messages in the cover text should avoid any changes in the original cover text to protect the stego text from suspicious. Regarding this, Jaro Wrinkler measurement can be used to measure the similarity between the two documents. Using the measurement, 1 means both documents are similar, while 0 means there are differences between them. Both syntactic and semantic methods are linguistic steganography which normally use substitution techniques (eg. punctuation or word replacement) to modify the originality of the cover text, which yields a suspicious stego text. More changes to the cover text will tend to be more suspicious and should be avoided. To avoid the OCR recognition tools or compression process destroying the hidden message, researchers use the alphabet properties to hide the hidden message such as CALP, CURVE, QUARD, VERT, Symmetric Reflection, and NCP. However, these approaches can hide less capacity of secret messages and also yield a suspicious stego text. The suspicion happens when there are changes against the cover text as illustrated below.

Secret Message : 1100
Cover Text : Ostrich is a bird. Ostrich can fly. So many types of birds are here. Peacock is our nation.
Stego Text : Ostrich is a bird. Peacock is our nation.

In the above example, the generated cover text is different than the stego text, which leads to suspiciousness. This has to be avoided.

NCP and Intelligent approach are capable to hide 4 bits of the secret message in one byte, which is able to push the capacity of hidden message. Therefore, a high number of bit can be embedded into a byte, which will increase the capacity rate ratio of the embedded secret message, using the formula below:

$$Capacity = \frac{size\ of\ secrete\ message\ (bits)}{size\ of\ cover\ text\ (bits)}$$

NCP approach uses character styles, which is Underline, Bold, Italic, and Arial to hide the hidden message bits. Four different character styles is used to map with 16 different values as shown in Table 3.

Font Type in Ms Word (FTMW) is another approach. It creates a table to represent the secret message using a font style. Some typefaces have a similar array of typeface such as Century: (Century 751BT; Century Old Style; Century Expd BT). This technique needs three capital letters of document to hide one symbol based on the corresponding type of font as shown in Table 4.

Table 3
Encrypted Table using NCP approach

Data Bits	Style			
	Underline (0/1)	Bold (0/1)	Italic (0/1)	Arial (0/1)
0000	x	x	x	x
0001	x	x	x	√
0010	x	x	√	x
0011	x	x	√	√
0100	x	√	x	x
0101	x	√	x	√
0110	x	√	√	x
0111	x	√	√	√
1000	√	x	x	x
1001	√	x	x	√
1010	√	x	√	x
1011	√	x	√	√
1100	√	√	x	x
1101	√	√	x	√
1110	√	√	√	x
1111	√	√	√	√

Table 4
Code Table for alphabets and space

Index	Characters	F1	F2	F3	Index	Characters	F1	F2	F3
1	A	1	1	1	16	P	2	3	1
2	B	1	1	2	17	Q	2	3	2
3	C	1	1	3	18	R	2	3	3
4	D	1	2	1	19	S	3	1	1
5	E	1	2	2	20	T	3	1	2
6	F	1	2	3	21	U	3	1	3
7	G	1	3	1	22	V	3	2	1
8	H	1	3	2	23	W	3	2	2
9	I	1	3	3	24	X	3	2	3
10	J	2	1	1	25	Y	3	3	1
11	K	2	1	2	26	Z	3	3	2
12	L	2	1	3	27	space	3	3	3
13	M	2	2	1					
14	N	2	2	2					
15	O	2	2	3					

FRMW approach yields a significant changes between the cover text and the stego text, which raises a suspiciosness as shown in Figure 3.


A New Digital Image Security Strategy: Steganoflage
Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt
School of Computing and Intelligent Systems, Faculty of Computing and Engineering. University of Ulster, Londenderry, Northern Ireland. United Kingdom
Johnny Depp, Robert De Niro, Kevin Spacey, Denzel Hayes Washington,
Russell Ira Crowe, John Travolta School of Computing and Intelligent Systems,
Faculty of Computing and Engineering. University of Ulster, Londenderry, Northern Ireland. UnitedKingdom
Email: Cheddad_A@email.ulster.ac.uk

Figure 3: Generated stego text using FRMW technique

Although the Jaro Winkler score equals to 1, but the human eye or computer system can detect the changes. Instead, the capacity of FRMW is very low with only 2.90% compared to the current score (7.04%) [32]. The changes of the cover text will raise the suspiciousness against eavesdroppers and computer system tools.

Intelligence approach divide 26 alphabets into two groups based on the height of characters by mapping bit 0 or 1 according to their groups as shown in Table 5.

Table 5
Intelligent Approach mapping bits

Bit	Character height	Group
0	LESS	a, c, e, i, m, n, o, r, s, u, v, w, x, z
1	LARGE	b, d, f, g, h, j, k, l, p, q, t, y

The table is used to generate a key and embed it into the cover text using RGB color value. Although the color is visually similar to each other, but it cannot defraud a computer system, which can easily detect the differences. Hence, the weakness of this approach lies in the changes of the color. This could lead to suspiciousness against the stego text by using a computer system tools.

Mathematical Model of Number System (MMNS) [33] is a new approach. It uses a number system. A formulae x * (x+1)/2 + y has been used to calculate the coordinate that represents each alphabet. In this technique, alphabets A to Z has been assigned with a corresponding coordinate as shown in Table 6.

Table 6
Coordinate representation for each alphabet

Alphabets	ASCII	*x*	*y*		Alphabets	ASCII	*x*	*y*
A	65	10	10		N	78	12	0
B	66	11	0		O	79	12	1
C	67	11	1		P	80	12	2
D	68	11	2		Q	81	12	3
E	69	11	3		R	82	12	4
F	70	11	4		S	83	12	5
G	71	11	5		T	84	12	6
H	72	11	6		U	85	12	7
I	73	11	7		V	86	12	8
J	74	11	8		W	87	12	9
K	75	11	9		X	88	12	10
L	76	11	10		Y	89	12	11
M	77	11	11		Z	90	12	12

In this technique, a word is represented using coordinates. Example below illustrates the representation for “ATTACK”.

A - 10,10
T - 12,6
T - 12,6
A - 10,10
C - 11,1
K - 11,9

A directed weight is generated to hide the secret message based on the obtained coordinate. Three disadvantages of this technique have been identified:

a) The coordinate of the alphabets is static or fixed.
b) The coverage of the coordinate is limited
c) This technique does not use any cover text in their implementation.

III. GENETIC ALGORITHM IN STEGANOGRAPHY

GA is the technique for optimization and searching, which is based on the principals of survival and reproduction. It has been used plentifully in information hiding for a few years and it was an effective technique for improving the performance of information hiding [17]. In steganography, GA is used particularly in images, audio and videos, but less used in text medium. This is because, the changes of stego object after embedding process using these media will not make a notable suspiciousness to human visual compared to text medium. According to [18], the changes of formatting and file size in text medium will increase the probability of being discovered by steganalysis tools and will lead to the reveal of the hidden message. Figure 4 shows the conceptual framework for applying GA in text steganography as proposed by [19].

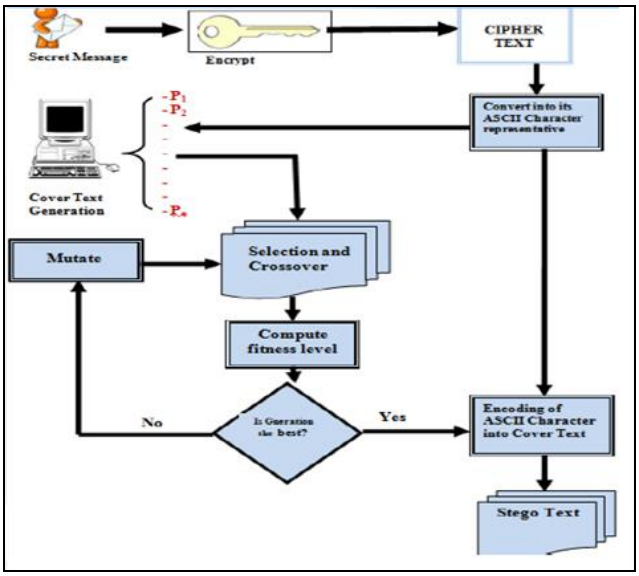

Figure 4: Conceptual Framework for applying GA proposed by [19]

LSB and MSB are the most famous two techniques used in steganography especially in images and audio because the changes do not raise the suspiciousness. Also, these two techniques are applied with several optimization techniques such as GA and DNA. Some studies found that GA can improve the performance of the stego object and that GA reduces the amount of error by using LSB technique and it improved the quality of images [34]. However, LSB and MSB techniques are not suitable for text steganography because they may alter the cover text and raise the suspiciousness. According to [19], GA approach is hard to attack by steganalysis because it uses a random number. GA can be applied together with text steganography as implemented by [11][19].

On the other hand, Genetic Algorithm-Based Model in Text Steganography (GATS) is one technique that replaces the last value of the ASCII code of the cover text with the hidden value. The technique is likely same as an LSB replacement, which is easy to implement, but has low imperceptibility [4] and is easy to detect by a steganalysis [35]. The proposed conceptual model is shown in Figure 4.

According to [36], out of 600 bytes of hidden message, only 424 bytes can be embedded into 1980 bytes of cover text although the capacity ratio for this technique is closed to 10%. The rest bytes of the hidden message require more than 1980 bytes of cover text to complete the embedding process.

The latest method in text steganography using GA is known as Crossover Encryption Based Text Steganography (CEBTS) [11]. It combines the random character sequence and feature coding method to hide a hidden message and generate a cover text. However, this technique embeds the hidden message in a random generated cover text, which tends to be suspicious. The hidden message is hidden at a sequence (j+pos) location, which is easy to detect by steganalysis system. The researcher claims that CEBTS can hide more than 70% of a plain text, which is far better than all existing approaches. Meanwhile, another advantage is that CEBTS reduces the time overhead. The robustness of this approach is still questionable since the overhead time is very less. This injection technique will increase the size of stego object and tends to raise suspiciousness. In short, the drawback of GATS and CEBTS are listed in Table 7.

Table 7
The Drawback and Future Work for GATS and CEBTS techniques

Technique	Drawbacks	Future Work
GATS	Used multiple cover text to generate a best one (not effective). The replacement of the last value will degrade the originality of cover text.	Focus on robustness and capacity of hidden message
CEBTS	Increase the size of cover text. Add the key into cover text at a sequence position (j + pos)	Use random technique

A study done by [37] shows that Multipoint, Diacritics, and MS Word Symbol algorithm do not change the file size and content of the cover text, avoiding the suspiciousness. However, these techniques are suitable for Arabic text (Arabic, Persian, Urdu) only.

According to [38], among the various information hiding, text steganography is difficult to hide information due to the redundant space to conceal a secret message. This is why most of the researchers prefer others medium compared to text medium. However, according to [14], text document remains to be an important choice due to its ubiquitous existence in the digital domain and is used for document tracking and copyright protection and authentication.

Among the available techniques, LSB is the most popular one and is widely used in image, audio and video due to its simplicity and large capacity. However, according to [4], LSB has low imperceptibility and low robustness, which can cause suspiciousness. A randomized LSB technique has been proposed to overcome the problem, where the next bit used in hiding message is selected based on some pseudo random techniques. GA has been used plentifully in information hiding discipline, especially in images and audio [39][40] and has been proven as an effective technique for improving the performance of information hiding systems. It is the basic theory of Evolutionary Algorithm (EA) used in computing for optimization and searching [41], which is based on the Darwinian principles of survival and reproduction [42].

Also, GA is used as an aiding tool for generating and optimizing security protocol [43]. It can be used to design a

general method to guide the steganography process to the best position for hiding data. According to [42] , GA can be used to increase the robustness of substitution techniques while maintaining the significant data hiding capacity [44].

Works on steganography have been rigorously reported. Hence, this study collects and reviews 98 papers between 2009 and 2013 on various steganography media (Figure 5) using GA. All of the papers are obtained from various databases such as IEEE, EBSCO host, Google Scholar, and Springer. The keywords such as genetic algorithm, crossover, mutation, and fitness are used to filter the related papers.

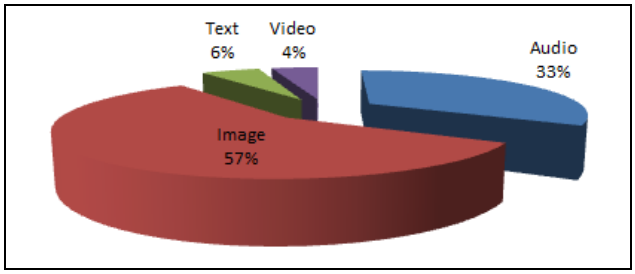

Figure 5: Percentage of Steganography Studies using Genetic Algorithm

The results show that most of the researchers focus more on image (57%) and audio (33%) media, and very less in video (4%) and text (6%) media. One of the reasons why researchers prefer to embed a hidden message into image and video is due to the plenty of redundant bits in these media compared to text medium. According to [45], redundant bits are the bits that can be altered without the alteration being detected easily.

LSB is the most frequently used technique in all media except text. The other techniques used are MSB, RSTEG, DCT, DWT, which is more suitable for images, audio, and video due to the huge number of redundancy space but not in text steganography. However, in text steganography, feature coding, changing syntax of the sentence and synonym of the word are the most popular techniques studied. The percentage show that there are less studies done in video and text steganography using genetic algorithm with only 4% and 6% respectively.

IV. Conclusion

Suspiciousness against stego text is very important in steganography to avoid third party detect the existence of secret message. There are numerous steganography studies focus on images, audio and video. However, there are less studies done in steganography using GA especially in video and text. LSB and MSB are the techniques for embedding messages in the stego object and are suitable for images, audio, and video. Based on the review, three gaps have been identified:

1. Most of the generated stego text produces a suspicious stego text which can be measured by Jaro Winkler measurement.
2. The secret message is embedded in a sequence order, which can be easily detect by text steganalysis. To reduce the detection rate, a randomized technique can be implemented during the steganography process.
3. Until today, the maximum 4 bits can hide in one a character. The number of hidden bits is expected to increase by manipulating an alphabet and using a mapping or placement technique.

Due to the limited redundant space in text medium, most of the researchers focus on the images and audio. However GA provides the optimization solution, hence it can be applied to text steganography, which is a very popular medium and uses less memory for communication compared to video steganography. In future, hiding a secret message using a random position without changing the cover text can be studied to avoid the changes and suspiciousness of stego text. MMNS can be enhanced to improve the stated weaknesses and can be integrated with GA to optimize the performance of stego text.

References

[1] C. P. Sumathi, T. Santanam, and G. Umamaheswari, "A Study of Various Steganographic Techniques Used for Information Hiding," *Int. J. Comput. Sci. Eng. Surv.*, vol. 4, no. 6, pp. 9–25, 2013.

[2] D.-C. Lou, J.-L. Liu, and H.-K. Tso, *Information Security and Ethics*. IGI Global, 2008.

[3] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *Computer (Long. Beach. Calif).*, vol. 31, 1998.

[4] S. Singh and A. Singh, "A Review on the Various Recent Steganography Techniques," *Int. J. Comput. Sci. Netw.*, vol. 2, no. 6, pp. 142–156, 2013.

[5] R. J. Anderson and F. A. P. Petitcolas, "On the limits of steganography," *IEEE J. Sel. Areas Commun.*, vol. 16, pp. 474–481, 1998.

[6] R. K. Tiwari and G. Sahoo, "A Novel Methodology for Data Hiding in PDF Files," *Inf. Secur. J. A Glob. Perspect.*, vol. 20, no. 1, pp. 45–57, 2011.

[7] R. Gupta, S. Gupta, and A. Singhal, "Importance and Techniques of Information Hiding : A Review," *Int. J. Comput. Trends Technol.*, vol. 9, no. 5, pp. 260–265, 2014.

[8] K. A. Kumar, S. Pabboju, and N. M. S. Desai, "ADVANCE TEXT STEGANOGRAPHY ALGORITHMS : AN OVERVIEW," *Int. J. Res. Appl.*, vol. 1, no. 1, pp. 31–35, 2014.

[9] E. Satir and H. Isik, "A compression based text steganography method," *Multimed. Tools Appl.*, vol. 70, no. 3, pp. 2085–2110, 2012.

[10] M. G. Vennice, M. Swapna, A. Ali, and T. D. Reddy, "A Hybrid Method of Hiding The Text Information Using Stegnography," *Int. J. Comput. Sci. Inform.*, vol. II, no. 1, pp. 160–164, 2012.

[11] K. Tarun, A. Pareek, J. Kirori, and Maninder Singh Nehra, *Development of Crossover and Encryption Based Text Steganography (CEBTS) Technique*, vol. 298. Springer New Delhi, 2014.

[12] B. Osman, R. Din, T. Zalizam, T. Muda, and M. N. Omar, "A Performance of Embedding Process for Text Steganography Method," *6th WSEAS World Congr. Appl. Comput. Conf. (ACC '13)*, pp. 115–119, 2013.

[13] D. D. Dhobale and V. R. Ghorpade, "An overview of advanced network protocol steganography," *Int. J. Adv. Res. Comput. Communiaction Eng.*, vol. 2, no. 9, pp. 2–5, 2013.

[14] L. Y. Por, K. Wong, and K. O. Chee, "UniSpaCh: A text-based data hiding method using Unicode space characters," *J. Syst. Softw.*, vol. 85, no. 5, pp. 1075–1082, 2012.

[15] A. M. S. Rahma, W. S. Bhaya, D. A. A. International, P. Abdul, M. S. Rahma, and D. A. Al-, "Text Steganography Based On Unicode of Characters in Multilingual," *Int. J. Eng. Res. Appl.*, vol. 3, no. 4, pp. 1153–1165, 2013.

[16] V. Saraswathi and S. Kingskin, "Different Approaches to Text Steganography: A Comparison," *Int. J. Res. Manag. Technol.*, vol. 9359, no. 11, pp. 124–127, 2014.

[17] I. Nechta and A. Fionov, "Applying statistical methods to text steganography," pp. 1–7, 2011.

[18] R. H. A. Rauf and N. H. Jamal, "Feasibility of Text Visualization in Text Steganalysis," in *New Trends in Software Methodologies, Tools and Techniques*, 2014, pp. 103–115.

[19] C. K. Mulunda and P. W. Wagacha, "Genetic Algorithm Based Model in

Text Steganography," *African J. Inf. Syst.*, vol. 5, no. 4, 2013.
[20] H. Yang and X. Cao, "Linguistic steganalysis based on meta features and immune mechanism," *Chinese J. Electron.*, vol. 19, no. 4, pp. 661–666, 2010.
[21] L. Xiang, X. Sun, G. Luo, and B. Xia, "Linguistic steganalysis using the features derived from synonym frequency," *Multimed. Tools Appl.*, vol. 71, pp. 1893–1911, 2014.
[22] G. S. Chandel, R. Gupta, and S. Jain, "Proposed Model of Dynamic Encryption using Steganography," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 2, no. 9, pp. 282–289, 2012.
[23] S. Bhattacharyya, P. Indu, S. Dutta, A. Biswas, and G. Sanyal, "Hiding Data in Text Through Changing in Alphabet Letter Patterns (CALP)," *J. Glob. Res. Comput. Sci.*, vol. 2, no. 3, 2011.
[24] S. Bhattacharyya, P. Indu, S. Dutta, A. Biswas, and G. Sanyal, "Text Steganography using CALP with High Embedding Capacity," *J. Glob. Res. Comput. Sci.*, vol. 2, no. 4, pp. 29–36, 2011.
[25] S. Kataria, B. Singh, T. Kumar, and H. S. Shekhawat, "PDAC (Parallel Encryption with Digit Arithmetic of Cover Text) Based Text Steganography," in *International Conference on Advances In Computer Sciences*, 2013, pp. 175–182.
[26] Shivani, V. K. Yadav, and S. Batham, "A Novel Approach of Bulk Data Hiding using Text Steganography," *Procedia Comput. Sci.*, vol. 57, pp. 1401–1410, 2015.
[27] C. Sunita, M. Peeyush, K. Tarun, and R. Sharma, "A Capital Shape Alphabet Encoding (CASE) Based Text Steganography," in *Conference on Advances in Communication and Control Systems*, 2013, vol. 2013, pp. 120–124.
[28] A. Majumder and S. Changder, "A Novel Approach for Text Steganography: Generating Text Summary Using Reflection Symmetry," *Procedia Technol.*, vol. 10, pp. 112–120, 2013.
[29] S. Kingslin and N. Kavitha, "Evaluative Approach towards Text Steganographic Techniques," *Indian J. Sci. Technol.*, vol. 8, no. November, pp. 1–8, 2015.
[30] S. Samanta, S. Dutta, and G. Sanyal, "A Novel Approach of Text Steganography using Nonlinear Character Positions (NCP)," *Int. J. Comput. Netw. Inf. Secur.*, vol. 6, no. 1, pp. 55–60, 2013.
[31] H. Singh and A. Diwakar, "An Intelligent Approach for Secure Data Transmission using Text Steganography," in *International Congress on Computer, Electronics, Electrical, and Coomunication Engineering*, 2014, vol. 59, pp. 13–17.
[32] E. Satir and H. Isik, "A Huffman compression based text steganography method," *Multimed. Tools Appl.*, vol. 70, no. 3, pp. 2085–2110, 2014.
[33] K. K. Mandal, A. Jana, and V. Agarwal, "A New Approach of Text Steganography Based on Mathematical Model of Number System," in *International Conference on Circuit, Power and Computing Technologies*, 2014, pp. 1737–1741.
[34] L. S. Jajo and S. S. Ghazoul, "Improving Hiding Information Process based on GA Technique with Secure Extraction Process In this paper we propose a new method of hiding information that produces a stego-image which is totally indistinguishable from the original image to extract the hid," vol. 10, pp. 98–106, 2010.
[35] P. C. Mandal, "An Extensive Review of Current Trends in Steganalysis," *J. Adv. Res. Comput. Eng. Technol.*, vol. 1, no. 7, pp. 215–220, 2012.
[36] S. Kataria, T. Kumar, K. Singh, and N. M. Singh, "ECR (Encryption With Cover Text and Reodering) based Text Steganography," in *Proceeding of the 2013 IEEE Seond International Conference on Image Information Processing*, 2013, pp. 612–616.
[37] A. Odeh, K. Elleithy, M. Faezipour, and E. Abdelfattah, "Highly efficient novel text steganography algorithms," *2015 IEEE Long Isl. Syst. Appl. Technol. Conf. LISAT 2015*, 2015.
[38] D. Bhattacharyya, A. Haveliya, and T.-H. Kim, "Secure Data Hiding in Binary Text Document For Authentication," *J. Appl. Math. Inf. Sci.*, vol. 8, no. 1L, 2014.
[39] S. C. Chu, H. C. Huang, Y. Shi, S. Y. Wu, and C. S. Shieh, "Genetic watermarking for zerotree-based applications," *Circuits, Syst. Signal Process.*, vol. 27, pp. 171–182, 2008.
[40] H.-C. Huang, J.-S. Pan, Y.-H. Huang, F.-H. Wang, and K.-C. Huang, "Progressive Watermarking Techniques Using Genetic Algorithms," *Circuits, Syst. Signal Process.*, vol. 26, pp. 671–687, 2007.
[41] M. N. Kumar and S. Srividya, "Genetic Algorithm based Color Image Steganogaphy using Integer Wavelet Transform and Optimal Pixel Adjustment Process," *Int. J. Innov. Technol. Explor. Eng.*, vol. 3, no. 5, pp. 60–65, 2013.
[42] M. Rana and R. Tanwar, "Genetic Algorithm in Audio Steganography," *Int. J. Eng. Trends Technol.*, vol. 13, no. 1, pp. 29–34, 2014.
[43] L. Zarza, J. Pegueroles, and M. Soriano, "Interpretation of binary strings as security protocols for their evolution by means of genetic algorithms," *Proc. - Int. Work. Database Expert Syst. Appl. DEXA*, vol. 0, pp. 708–712, Sep. 2007.
[44] N. Cvejic and T. Seppanen, "Increasing the capacity of LSB-based audio steganography," *2002 IEEE Work. Multimed. Signal Process.*, 2002.
[45] P. Kumar and V. K. Sharma, "Information Security Based on Steganography & Cryptography Techniques : A Review," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 4, no. 10, 2014.