Indonesian Journal of Electrical Engineering and Computer Science
Vol. 11, No. 2, August 2018, pp. 768~774
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v11.i2.pp768-774

A Comparative Review on Data Hiding Schemes

Roshidi Din[1], Raihan Sabirah Sabri[2], Aida Mustapha[3], Sunariya Utama[4]
[1,2,4]School of Computing UUM College Arts and Sciences, Universiti Utara Malaysia, 06010, Sintok, Kedah, Malaysia
[3]Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, Parit Raja, 86400 Batu Pahat, Johor, Malaysia

Article Info

Article history:

Received Apr 1, 2018
Revised Jun 20, 2018
Accepted Jul 7, 2018

Keywords:

Data hiding.
Decoding scheme
Decrypting scheme
Extracting scheme

ABSTRACT

Data hiding is a technique used to protect confidential information. The aim of a particular data hiding scheme is to make a more secure and robust method of information exchange so that confidential and private data can be protected against attacks and illegal access. The aim of this paper is to review on different data hiding schemes, covering the decoding, decrypting and extracting schemes. This paper also highlighted three major schemes that are widely used in research and real practice. The discussion include findings on the most recent work on decryption schemes.

Corresponding Author:

Roshidi Din,
School of Computing UUM College Arts and Sciences,
Universiti Utara Malaysia, 06010, Sintok, Kedah.
Email: roshidi@uum.edu.my

1. INTRODUCTION

The rapid growth of the Internet communication calls for a specialization on security of computers network. It is imperative to protect the confidentiality and integrity of the data transmitted against unauthorized access [1]. Security and privacy issues of the transmitted data have also become an important concern in multimedia applications. This has led to the introduction of numerous novel schemes in the field of steganography and cryptography with the goals of improving security, reliability, and efficiency [2].

For instance [3] stated that the improvement in term of authentication schemes brought to smart card more protected and safe have been proposed. Evidently various schemes had suggested to overcome the current situation where the deficiency of secured. Usually previous researcher belive their scheme could endure numerous attacks [3]. Unfortunately not all the previous scheme could be withstand the attack.Only the capable schems can be dealing.

In general, there are three main methods of information security being used; steganography, cryptography and watermarking. Steganography is a process hiding a secret message with cover message and transmit to recipient without others parties realizes the existing hidden message. It can be applied in images, text, audio, and video [4]. It is known as process to conceal secret message intended for invisible communication. In order to safely transmit information, steganography technique can be used to prevent the knowledge of the existence of secret communication between sender and receiver [5].

Meanwhile, cryptography is essentially secret writing. A cipher is a secret method of writing, where by plaintext is transformed into a cipher text. In cryptography, it is easy to found that the text consist of secret information. Cryptography shows the way to protect the content of information where originator of message is encrypted using key and shares the secret information. Receiver extracts the secret information using (key) decryption algorithm. This key can be either symmetric or asymmetric. Cryptography techniques are based on rendering the content of a message garbled to unauthorized people [6].

Then, in watermarking, data are hidden to convey some information about the cover medium such as ownership and copyright. This is carried out by inserting text or logo in digital media such image, audio and video. The three methods of information security is similar in the sense that implementation begin with securing process to cover the important data in order to hide the hidden information or securing the availability data.

In the previous research, the securing processes are mostly in the form of encoding, encrypting and embedding process. Afterwards, the last implementation mostly is how to generate the secured data based on data before the securing process. This includes decoding, decrypting, and extracting the secret text or messages.

The remainder of this paper is organized as follows. Section 2 presents the review category of the data hiding schemes, Section 3 presents the trends of the data hiding interpreted schemes, Section 4 presents the preferred data hiding schemes and finally Section 5 discusses the reviews and concludes the paper.

2. REVIEW CATEGORY

This paper reviews different types of data hiding schemes that consist views from decoding, decrypting and extracting process. Information decoding is the process to convert a cyphered text back to plain-text while decrypting is taking an encrypted text and converting it back into original text. Meanwhile, extracting is the process of converting the cipher text into the plain text by using a secret key. Table 1 shows the classification of schemes based on the literature from the last decade.

Table 1. Classification of Schemes

Type	Schemes	Symbol Representation
Decoding Schemes	Neural-based Poetry Generation [4]	neuralB
	Arbitrary Algorithm Encryption [5]	AAE
	Encoding Hiding the Message into An Excel Graph [6]	EXCELg
	RJDA Algorithm [7]	RJDA
	Alphabet Index Matrix (English & Malayalam) [8]	ALPHAiM
	Encoding of Hindi Text [9]	EnHindiT
	Visual Cryptography Schemes [10]	VCrypS
	Homomorphic Encryption Scheme [11]	HES
	A Boots Trappable Encryption Scheme [12]	trapEnS
	Huffman Coding Algorithm [13]	HCA
	Elliptic Curve Cryptography(Ecc) [14]	ECC
	DWT Domain of A Carrier Image [15]	DWT
	Watermark [16]	Ws
Decrypting Scheme	Encapsulation Schemes [17]	ENCAPs
	Hybrid Scheme [18]–[21] [18]	HS
	Advance Encryption Standard (AES) [22]–[25]	AES
	Rivest-Shamir-Adlema Algorithm (RSA) [11], [18], [19], [26]	RSA
	Data Encryption Standard (DES) [23], [27]	DES
	LSB [5], [12], [28]	LSB
	Homomorphic Encryption Scheme [21], [22], [26]	HES
	Conventional Encryption Algorithms Blowfish [23]	CEABW
	Binary RSA Encryption Algorithm (BREA) [19]	BREA
	Symmetric Key Encryption [23], [29], [30]	SKE
	RDH Schemes [31]	RDH
	Huffman Encoding Algorithm [28]	HEA
	Transposition Cryptography Algorithm [32]	TCA
	A Boots trappable Encryption Scheme [12]	BTRS
	ECC Decryption [14]	ECC
	ECR (Encryption with Cover Text and Reordering) [33]	ECR
Extracting Schemes	STC (Syndrome-Trellis Code) Scheme [34]	STC
	Compression Algorithm [35]	CA
	Random Character Scheme [36]	RC
	Hide Text-In-Text Messages [37]	HTTM
	Web Text Extraction [38]	WTE
	Extract The Chinese Text [38]	ECT
	Hybrid Algorithm [39]	HA
	RDH Scheme [40]	RDH
	Blowfish Algorithm [40]	BWA
	Bwt (Burrows Wheeler Transform)	BWT
	HHK Encoding (Hindi Hexadecimal Modified Katapayadi Encoding) Scheme [41]	HHK
	Advanced Data Encrypt (AES) [42]	AES
	Data Encryption Standard (DES) [36]	DES
	Rivest-Shamir- Adleman Algorithm [43]	RSA
	L-R Schemes [44]	L-R
	Simple Text Embedding Scheme With Reversibility [43]	STESR

Based on Table 1, the three types of schemes criteria are supplemented with symbol representation. Firstly, there are 14 decoding schemes available listed as a result of relevant search studies, for example Neural-based poetry generation such as neuralB, AAE, EXCELg, RJDA, ALPHAiM, EnHindiT, VcrypS, HES, trapEnS, HCA, ECC, DWT, Ws, and ENCAPs. Secondly, there are 15 decrypting schemes available listed as a result of relevant search studies, for example the HS, AES, RSA, DES, LSB, HES, CEABW, BREA, SKE, RDH, HEA, TC, BTRS, EE, and ECR. As for the extracting scheme, there are 16 schemes listed, for instance STC, CA, RC, HTTM, WTE, ECT, HA, RDH, BWA, BWR, HHK Encoding, AES, DES, RSA, L-R Schemes, and STESR.

3. TRENDS OF DATA HIDING SCHEMES

Once the data hiding schemes in decoding, decrypting and extracting have been identified, this paper reviews the implementation trend based on several years of research effort on data hiding. The trends are measured based on the most frequently used schemes in the respective categories.

3.1. Decoding Schemes

Figure 2 illustrates the number of literature specific to decoding schemes since 2001 until 2017. The most noticeable thing about Figure 1 is that, the number of studies on decoding schemes is moderate from the beginning until now. It is not applicable to choose the most used decoding schemes because each schemes type have only one contribution for each studies throughout the last decade. The trends also showed that new schemes are introduced almost on yearly basis. The literature also showed that there are substantial number of new schemes proposed under the decoding schemes. The research on encoding schemes begin from ENCAPs (2001), Ws (2006), DWT (2007), HCA (2010), ECC (2010), HES (2011), trapEns (2011), VCrypS (2012), EnHindiT(2014), ALPHAiM (2015), AAE (2016), EXCELg (2016), RJDA (2016), and finally the latest scheme called neuralB (2017).

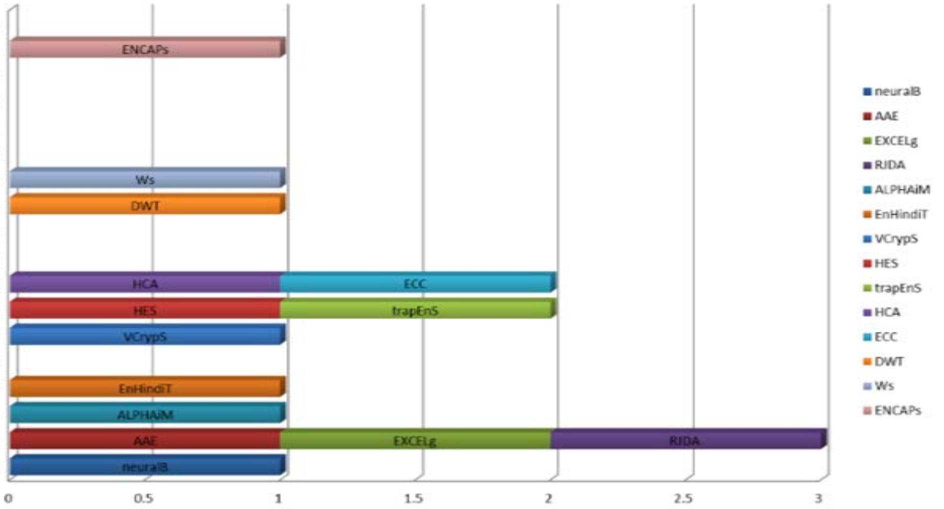

Figure 1. Trends of decoding schemes

Furthermore, Figure 1 demonstrates that the research on decoding schemes became aggressive during 2016, where three contributions of study findings were made throughout that year. Next was back in 2010 and 2011 when HCA, ECC, HES, and trapEnS were introduced. Other years showed consistent but small contribution made every year, thus indicating that the studies in terms of decoding schemes are very much lacking.

3.2. Decrypting Schemes

Decrypting schemes consists of 15 schemes type as listed in Table 1. Figure 2 shows the research pattern in decrypting schemes within 10 years since 2008. In this figure, the development of schemes in research is growing since 2014, perhaps the awareness of the importance of study schemes is begun. Starting in 2014, the development of schemes is increasingly rising with various research schemes produced every year. There were three types of schemes being studied during the year. Years later, two new schemes were introduced in 2015.

Moving towards 2017, the figure shows that the research trend is proposding a new scheme each year, rather than improving the performance of the schemes available from the literature. The most aggressive year is 2016 with the introduction of 11 different new schemes being proposed. Nonetheless, the following year showed a sudden decline in research on decrypting scheme.

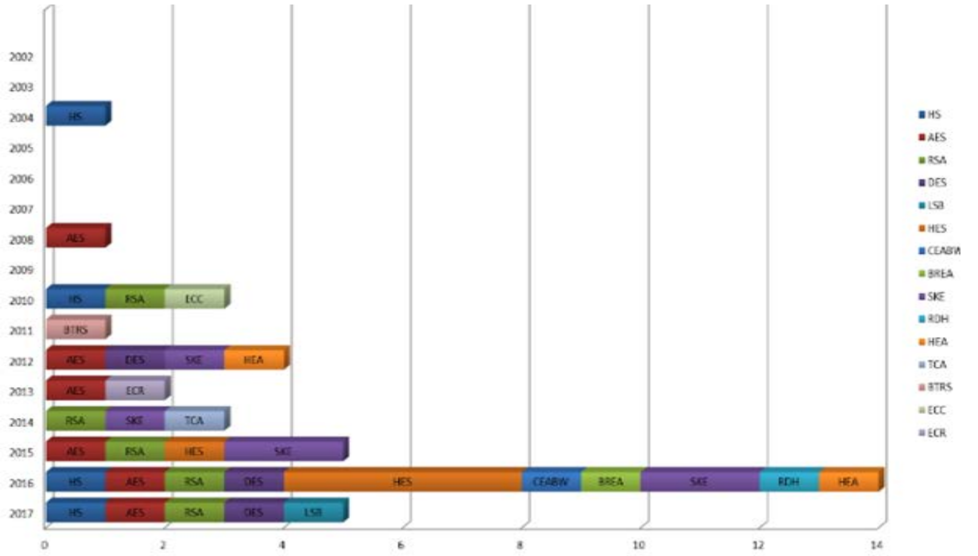

Figure 2. Trends on decrypting schemes

3.3. Extracting Schemes

The extracting schemes consist of 16 schemes type as listed in Table 1. Figure 2 shows that introduction of existing schemes are moderate since 2011 throughout the last 10 years. Based on this figure, extracting schemes were first introduced in 2011 but not work has contributing to the area until 2014. In 2014, the development of schemes in research is growing gradually; perhaps due to the awareness of the importance of study schemes. There were seven types of schemes proposed in 2014. 2015 saw a decline in the study but increased again in 2016. Referring to the graph, it can be concluded that a new extracting scheme is proposed every year.

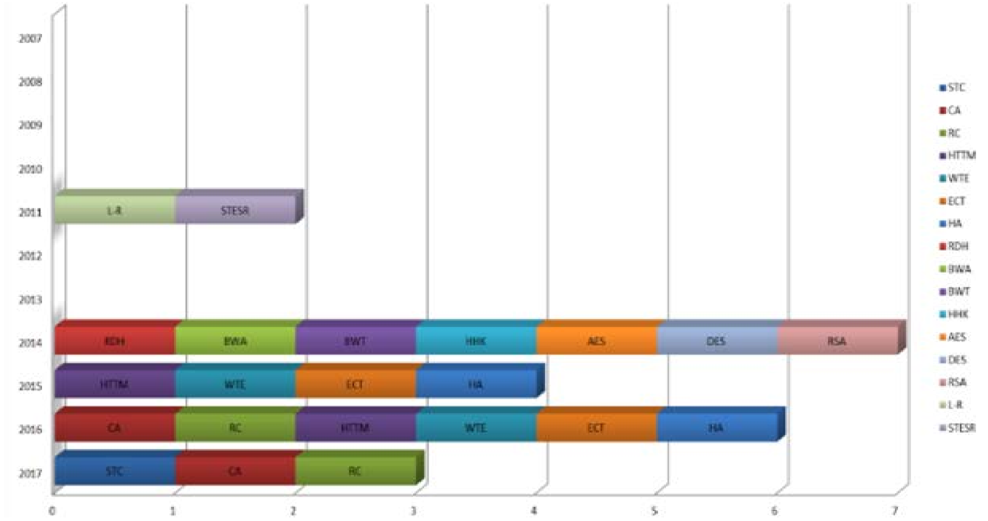

Figure 3. Trends on extracting schemes

The lack of research in related schemes makes it difficult to identify the schemes that are ranked top among all the 16 underlying schemes as listed. Based on the graph, most aggressive year of research on extracting scheme was back in 2014. The year 2016 is in the second place followed by the year 2015, with 4 research studies. It is clear that the year was between years of non-aggressive study. Based on the pattern showed by Figure 3, the study on extracting schemes is not encouraging. The most widely used schemes are as CA, RC, HTTM, WTE, ECT, and HA as compared to other schemes.

4. PREFERRED DATA HIDING SCHEMES

Given the trends of research on data hiding schemes in the last decade, Figure 4 to Figure 6 shows the preference on data hiding interpreted schemes based on literature review in previous section. First, Figure 4 shows two groups of patterns, where the first group is among the widely used aspects, the second group is among the fewest groups. The figure also show a small gap of difference between each schemes type.

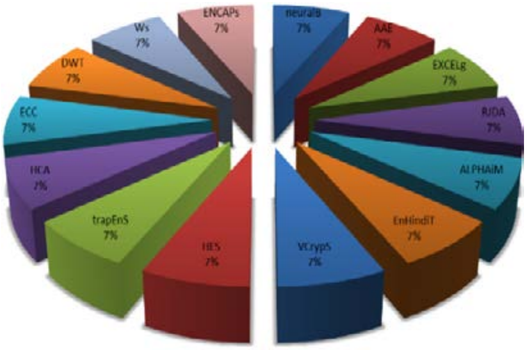

Figure 5. Preferred decrypting schemes

Symmetric Key Encryption (SKE) techniques are used to provide security at higher levels. The main advantage of SKE is that management of the key is very simple and easy since only one key is needed. SKE can take input data in sentence format, which provides a very much secure system with less vulnerability to cryptanalyst attacks. Utilizing a combination of the AES schemes of encryption/decryption along with visual cryptography, one can ensure the highest form of security. The AES is substantial secure through its variable key and structure. SKE and AES became the main schemes option to researcher compared with other schemes. But for others schemes types can be determine as the most rarely used.

Finally, Figure 6 shows the preferred extracting schemes from the literature. The findings showed that majority of the previous research used CA, RC, HTTM, WTE, and ECT and HA (9%) as compared to STC, RDH, BWA, BWT, HHK, AES, DES, RSA, L-R and STESR, which are 5% each. The figure also showed that the development of schemes are quite slow based on findings of the literature review results.

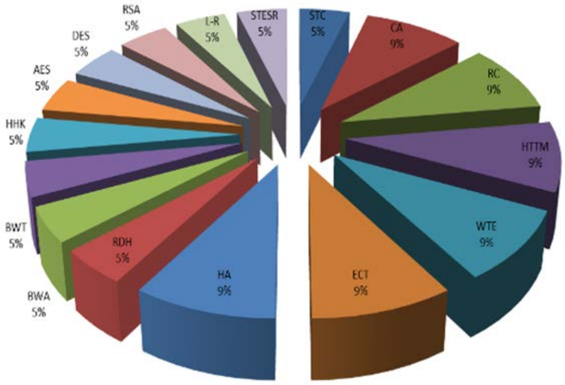

Figure 6. Preferred extracting schemes

5. DISCUSSION AND CONCLUSIONS

This paper reviews interpreted data hiding schemes used in data in recent years, which are decoding, decrypting and extracting schemes between 2001 until 2017. The most noticeable finding for decoding schemes is that the number of studies is moderate throughout the decade. In general, only one algorithm is proposed in each year. Furthermore, the study demonstrates that the research becoming aggressive beginning 2016 with three contributions in the year.

As for the decrypting schemes, the most widely used in decryption schemes with the highest number of studies in data hiding are shown in Figure 7 with 15% SKE, 15% AES, 13% RSA, and 13% HES. Meanwhile for the year of aggressive research is occurs in 2016 with 15 studies.

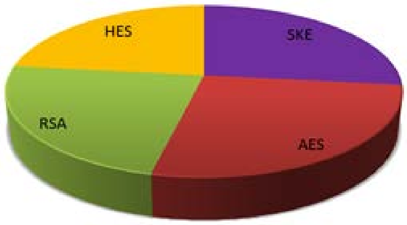

Figure 7. Highest decrypting schemes used

Finally, for the extracting scheme, the highest number of studies in data hiding is shown in Figure 8, which include the compression algorithm (CA), random character scheme (RC), hide text-in-text messages (HTTM), web text extraction (WTE), extract the Chinese text (ECT) and hybrid algorithm (HA). All these schemes are sharing the same amount of literature studies finding. Therefore it makes these schemes is the frequently used group of schemes. Meanwhile, the research on this scheme was aggressive in 2014 with 7 newly proposed extracting schemes.

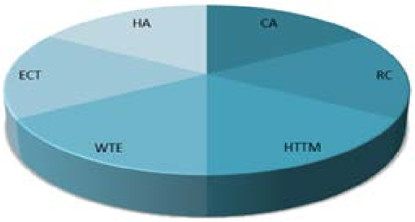

Figure 8. Highest extracting schemes used

As the conclusion, this review is a useful evaluation for researcher to identify the most widely-used data hiding interpretation and enable the researchers to choose the trend of interest in presenting a new encoding, decrypting or extracting schemes.

ACKNOWLEDEMENT

This research is jointly supported by the Fundamental Research Grant Scheme (FRGS), MoHE under SO Code 13576 Universiti Utara Malaysia and Vot 1557 Universiti Tun Hussein Onn Malaysia.

REFERENCES

[1] R. F. Mansour, W. F. Awwad, and A. A. Mohammed, “A Robust Method to Detect Hidden Data from Digital Images,” vol. 2012, no. April, pp. 91–95, 2012.
[2] S. Dey and A. Abraham, “Data Hiding Techniques Using Prime and Natural Numbers,” pp. 1–45.
[3] H. Tu, “A Security Enhanced Password Authentication and Update Scheme Based on Elliptic Curve Cryptography,” vol. 12, no. 10, pp. 7353–7360, 2014.
[4] Y. Luo and Y. Huang, “Text Steganography with High Embedding Rate,” Proc. 5th ACM Work. Inf. Hiding Multimed. Secur. - IHMMSec ’17, pp. 99–104, 2017.

[5] I. Azad, “A New Method for Text Hiding in the Image by Using LSB,” vol. 7, no. 4, pp. 126–132, 2016.

[6] F. Akhter, “A Secured Word by Word Graph Steganography using Huffman Encoding,” pp. 9–12, 2016.

[7] O. W. Liang and V. Iranmanesh, “Information Hiding using Whitespace Technique in Microsoft Word,” 2016.

[8] P. M. Vidhya and V. Paul, *“A method for text steganography using malayalam text,”* Procedia Comput. Sci., vol. 46, no. Icict 2014, pp. 524–531, 2015.

[9] R. Shah and Y. S. Chouhan, “Encoding of Hindi Text Using Steganography Technique,” no. 1, pp. 22–28, 2014.

[10] K. Tsan and L. Author, “Based on Binary Encoding Methods and Visual Cryptography Schemes to Hide Data,” pp. 4–7, 2012.

[11] M. Hong, W. Zhao, and P. Wang, “Homomorphic Encryption Scheme Based on Elliptic Curve Cryptography for Privacy Protection of Cloud Computing,” 2016.

[12] Z. Brakerski, “Efficient Fully Homomorphic Encryption from (Standard) LWE,” pp. 97–106, 2011.

[13] K. Negrat, R. Smko, and A. Almarimi, “Variable Length Encoding in Multiple Frequency Domain Steganography,” pp. 305–309, 2010.

[14] P. Bh, D. Chandravathi, and P. P. Roja, “Encoding And Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz ’ s Method,” vol. 2, no. 5, pp. 1904–1907, 2010.

[15] S. Yang, “Text Information Hiding Method Based on Chaotic Map and BCH Code in DWT Domain of A Carrier Image,” pp. 239–241, 2007.

[16] M. A. Qadir and I. Ahmad, “Digital Text Watermarking : Secure Content Delivery and Data Hiding in Digital Documents,” no. November, pp. 18–21, 2006.

[17] P. R. Bellare, Mihir, “Encode-then-encipher encryption: How to exploit nonces or redundancy in plaintexts for efficient cryptography,” 2001.

[18] D. Jpdlo, F. R. P. Ghrovdwyhhu, and J. Frp, “A Hybrid Technique of Cryptography and Watermarking for Data Encryption and Decryption.”

[19] D. John and L. Martin, “Binary rsa encryption algorithm,” pp. 178–181, 2016.

[20] A. Khan, K. K. Mishra, N. Santhi, and J. Jayakumari, “A New Hybrid Technique for Data Encryption,” no. Gcct, pp. 925–929, 2015.

[21] W. U. Xing-hui, “Research of the Database Encryption Technique Based on Hybrid,” pp. 82–85, 2010.

[22] S. Rao, “A Novel and Highly Secure Encryption Methodology using a Combination of AES and Visual Cryptography,” pp. 1682–1688, 2016.

[23] R. Yegireddi, “A survey on Conventional Encryption Algorithms of Cryptography,” 2016.

[24] A. Azougaghe, Z. Kartit, M. Hedaboui, M. Belkasmi, and M. E. L. Marraki, “An efficient algorithm for data security in cloud storage,” 2016.

[25] A. Jain, “Encrypted Reversible Data Hiding on Compressed Image,” vol. 69, no. 25, pp. 1–5, 2013.

[26] R. Minni, K. Sultania, S. Mishra, P. Durai, and R. Vincent, “An Algorithm to Enhance Security in RSA,” pp. 4–7, 2013.

[27] B. Karthikeyan, A. It, and V. College, “A Combined Approach of Steganography with LSB Encoding technique and DES Algorithm,” pp. 1–4, 2017.

[28] M. V Kale and P. S. A. Patil, “Text Hiding In Multimedia By Huffman Encoding Algorithm Using Steganography,” vol. 2, no. 1, pp. 1–5, 2016.

[29] R. Sultana and T. M. Kumari, “An ASCII Value based Optimized Text data,” pp. 6650–6656, 2016.

[30] U. Singh and U. Garg, “An ASCII value based text data encryption System,” vol. 3, no. 11, pp. 1–5, 2013.

[31] F. Huang, J. Huang, and Y. Shi, “New Framework for Reversible Data Hiding in Encrypted Domain,” vol. 11, no. 12, pp. 2777–2789, 2016.

[32] N. Bhopal, “Transposition Cryptography Algorithm using Tree Data Structure,” no. 978, 2014.

[33] S. Kataria, T. Kumar, K. Singh, and M. S. Nehra, *“ECR (encryption with cover text and reordering) based text steganography,”* 2013 IEEE 2nd Int. Conf. Image Inf. Process. IEEE ICIIP 2013, pp. 612–616, 2013.

[34] M. Y. Elmahi and M. H. Sayed, “Text Steganography Using Compression and Random Number Generators,” vol. 6, no. 6, pp. 259–263, 2017.

[35] S. Chaudhary and M. Dave, “An Elucidation on Steganography and Cryptography,” pp. 3–8, 2016.

[36] [A. P. Kaur and G. Singh, “INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY Designing and Performance Evaluation of Text Data Hiding Technique Using Sequential Encoding and Decoding Technique,” vol. 3, no. Ii, pp. 6–11, 2015.

[37] A. Hamarsheh, “Exploiting Omega Networks to Hide Text-in-Text Messages,” vol. 15, no. 5, pp. 39–43, 2015.

[38] R. Guo, J. Qiu, and G. Zhang, “Web-based Chinese term extraction in the field of study,” 2015.

[39] H. Huanhuan, Z. Xin, Z. Weiming, and Y. Nenghai, “Adaptive Text Steganography by Exploring Statistical and Linguistical Distortion,” 2017.

[40] S. Sreekumar and V. Salam, “Advanced Reversible Data Hiding With Encrypted Data,” vol. 13, no. 7, pp. 310–313, 2014.

[41] P. Bharti and R. Soni, “A New Approach of Data Hiding in Images using Cryptography and Steganography,” vol. 58, no. 18, pp. 1–5, 2012.

[42] M. P. Uddin, M. Saha, S. J. Ferdousi, M. I. Afjal, and M. A. Marjan, “Developing an efficient solution to information hiding through text steganography along with cryptography,” 2014 9th Int. Forum Strateg. Technol. IFOST 2014, pp. 14–17, 2014.

[43] A. T. Abbasi and B. Ahmad, “Urdu text steganography : Utilizing isolated letters,” vol. 2015, pp. 37–46, 2015.

[44] C. Lin, L. Yang, and Y. Chen, “Data Hiding Scheme based on Features of Chinese Text,” pp. 0–3, 2011.