Journal of Computer Engineering
ISSN 10003428

Original Research Article
Vol 10, Issue 1, 2021 | ISSN: 1000-3428

# Advanced Cryptographic Techniques for Concealing Data within Microsoft Word Documents

**Dr. Sophia Patel, Dr. Ethan Thompson**

*Dr. Sophia Patel, Department of Computer Science, University of California, Berkeley; Dr. Ethan Thompson, School of Information Technology, Carnegie Mellon University.*

***Abstract*—**Seamless modification of an entity for the purpose of hiding a message of significance inside its substance in a manner that the embedding remains oblivious to an observer is known as steganography. Together with today's pervasive registering frameworks, steganography has developed into a science that offers an assortment of strategies for stealth correspondence over the globe that must, however, need a critical appraisal from security breach standpoint. Microsoft Word is amongst the preferably used word processing software, which comes as a part of the Microsoft Office suite. With a user-friendly graphical interface, the richness of text editing, and formatting topographies, the documents produced through this software are also most suitable for stealth communication. This research aimed not only to epitomize the fundamental concepts of steganography but also to expound on the utilization of Microsoft Word document as a carrier for furtive message exchange. The exertion is to examine contemporary message hiding schemes from security aspect so as to present the explorative discoveries and suggest enhancements which may serve a wellspring of information to encourage such futuristic research endeavors.

## I. Introduction

THE word "information" alludes to a free antiquity portrayed by the reliant connections between various events [1]. For this study, it is treated as an element of significance (in plain or encrypted form) that is ought to be given a cover against unauthorized revelation.

The arrangement of two Greek words στεγανός (steganos: signifying "cover") and γράφειν (graphein: representing "composing") constitutes what alluded to as steganography [2]. It is one of the four essential subdivisions of the field called information hiding as outlined in Fig. 1 [3], which is an augmentation of [4], and its single drive is to guarantee the covering of the presence of the concealed data [5].

Current computerized steganography takes advantage of the confinement of human aural and visual frameworks [6]. It is so since human discernable limits fall somewhere around 20 and 20,000 Hz [7]. Interestingly, human's visionary framework as discovered is constrained by constituents, for example, the field of view, precise determination, the blind side, and the visible range [8]-[11]. Subsequently, it is basic that a clamor underneath the noticeable range stays undetected paying little mind to it to be altered or not. Similarly, a visual entity, for example, a picture is probably going to cross undetected upon examination by the naked eye in the domain of the chromatic human confinements.

This research, restricted to the security analysis of the steganographic schemes proposed for the Microsoft (MS) Word document, aimed at signifying the role and usage of stego key in achieving confidentiality. Rest of the paper takes the form as follows:

Section II elucidates on a short historical background of steganography. The dialect, types, model, strategies, assessment criteria and various genera of assaults on steganographic systems are the subjects of Section III. Literature review covered in Section IV. A novel steganography scheme utilizing MS Word document is the focus of Section V. Section VI clarifies the examination discoveries assembled while investigating the targeted steganographic strategies. Section VII sums up the discussion.

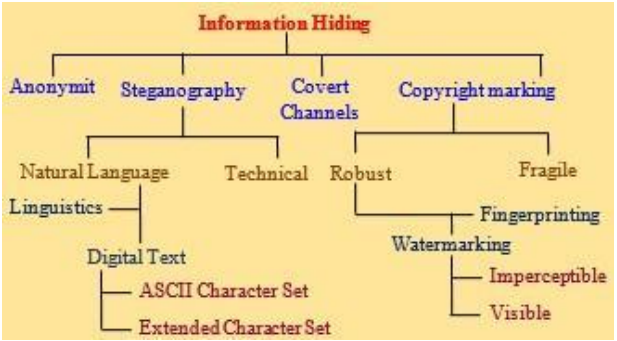


Fig. 1 Classification of information hiding [3], [4]

## II. Brief History of Steganography

Despite the fact that the fifteenth-century finale saw the coining of the word steganography, its utilization by Herodotus goes back to 440 BC. Histiaeus composed a secret message on the shaved scalp of his most trusted worker held up till his hair grew and afterward conveyed the message by sending him to his partners where his head was re-shaved to uncover the message. Demaratus composed a note on the wooden surface of the wax composing tablet and after that covered it with wax. From the youngsters using orange juice as invisible ink for


How to cite: Dr. Sophia Patel, Dr. Ethan Thompson (2021). Advanced Cryptographic Techniques for Concealing Data within Microsoft Word Documents. Journal of Computer Engineering, 10(1), 15–24. DOI: https://doi.org/10.5281/zenodo.19342477

mystery composing (for no particular reason) to (hazardous) covert exercises by spies and psychological oppressors and the utilization of Microdot by Germans in World War II [12]-[16] are some other protuberant references from the past.

## III. Dialect, Types, Model, Strategies, Appraisal Criteria and Types of Assaults on Steganographic Systems

### A. The Dialect

The language/terminology [17] used to discuss steganography alongside its brief explanation follows next and is diagrammatically shown in Fig. 2:

1) *Message:* Contents of importance that need camouflage.
2) *Cover:* The carrier used for concealing a message.
3) *Embedding:* Hiding of the secret message inside the selected cover or message bearer.
4) *Stego Object:* It is the altered cover after message inserting.
5) *Extraction:* Taking the embedded data out of the stego object.
6) *Stego Key:* An element that coordinates the procedure of message inserting inside cover and its ensuing extraction from stego object.
7) *Steganographic System:* The method of message implanting at the sender's end, the transmission of the stego object over the insecure channel, and the extraction of the installed message at the receiver's end constitutes a total steganographic framework.

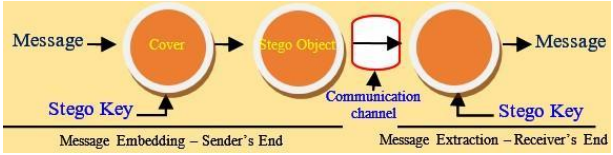


Fig. 2 Steganographic system

### B. Categories of Steganography

The three classes of steganographic frameworks [18] include:

1) *Pure:* This class incorporates routine steganographic frameworks that operate without a stego key. Thus, this sort is additionally the weakest giving the supposition that nobody other than those in communication knows about such stealth exchange of message.
2) *Symmetric/secret:* It incorporates steganographic frameworks that utilize a stego key for message embedding. The restriction, notwithstanding, is that the addressee of the stego object should likewise have the same stego key for message extraction.
3) *Asymmetric/public:* Steganographic systems having a place with this sort use a pair of stego keys where message embedding is done utilizing a private piece of stego key-pair, while hidden message extraction is done using public part of the stego key.

### C. Models for Steganography

Simmons [19] spearheaded the displaying of present day steganographic convention where Alice and Bob kept in isolated cells in detainment needed to arrange their escape. They were permitted for message exchange, however, just through superintendent Wendy who could hinder the correspondence if there should arise an occurrence of anxious informing. Henceforth, Alice could speak with Bob, utilizing the pre-concurred parameters before getting held, with some drawing showing the escape arrange. Alice could then modify it, as an improvement, to demonstrate her perspective without getting it seen by Wendy.

Instant messaging/communication through the Internet, for example, impacts the attitude of allies (from credulous to master) towards data security mindfulness [20]. The same, likewise, has secretly infiltrated in the modeling of communication accords as it is evident from the steganographic model proposed by [21] as shown in Fig. 3, to manage known cover assaults (addressed in the following section).

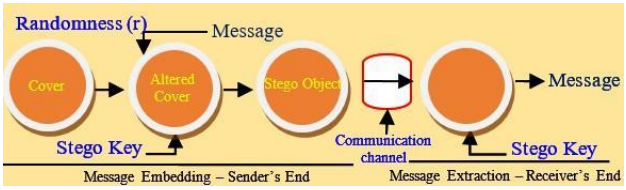


Fig. 3 Model for secure steganography

### D. Techniques Used in Steganography

Steganographic practices include the following or any of their hybrid compositions [22] as shown in Fig. 4. In any case, considering the extent of this study, just the related methods of insertion/injection or substitution are taken for discussion here. [3] is suggested as a suitable reference for the understanding of remaining techniques.

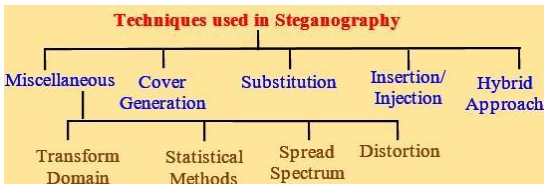


Fig. 4 Different types of steganographic techniques

1) *Insertion/Injection:* Here, the message gets embedded as a part of the cover, for example, infusing message after the end of file mark (EOF) [23]. As obvious, the incite impediment is the expanded size of stego object

that can point towards the veiled message when contrasted with the real cover.

2) *Substitution:* Embedding is done either by supplanting or substituting the substance of the chosen cover with that of the message. The detectable quality of the stego object, nonetheless, is the first sympathy toward this strategy.

3) *Cover Generation* 4) *Hybrid Approach*

5) *Miscellaneous:* Encompassing but not just limited to the following approaches:

- Transform Domain ☐ Spread Spectrum
- Statistical Methods ☐ Distortion

*E. Evaluation Criteria*

Capacity, security, and robustness are the evaluation criteria in [24], whereas [25] focused on perceptibility, integrity, and robustness. Because capacity, integrity, perceptibility, and robustness contribute towards ensuring secrecy of cover used, these parameters are selected as the gauging parameters for the targeted steganographic schemes. Security, however, is the protection resulting by adhering to the laid down policies and procedures that govern communication, and hence, it is discussed at length in Section V. Fig. 5 is the diagrammatic representation of this idea.

Fig. 5 Gauging parameters for secure steganography

*F. Types of Assault on Steganographic Systems*

The subdivision of science that is concerned with finding and extracting out the message covered up inside the stego object without the knowledge of stego key is known as steganalysis [26]. Thus, the awareness about the assaults propelled against an appropriate steganographic framework is obligatory. Furthermore, it also adds proficiency and efficacy in the scheming of a new or enrichment of prevailing steganographic system. It is desirous to apprehend that, when the purpose of an assault is to mutilate or destroy the concealed message, it is called an *active*. However, when the only concern is to know about the disguised substance, then that type of attack is referred to as a *passive* attack [27]. It is worth specifying that an aggressor can commit two kinds of errors [28] while examining a stego object as follows:

1) *False Positive:* The attacker catches an entity as a carrier of concealed message which in reality is not the case.

2) *False Negative:* The assailant leaves an entity unscrutinized which in fact is a bearer of the secret message.

The five types of assaults on a steganographic framework [29] abridged as follows:

- Stego only attacks_ The assailant has access to stego object and tries to investigate and remove the concealed message.
- Known Cover attack_ The aggressor having the learning of the stego object and the cover utilized endeavors to differentiate these for getting the hidden message.
- Known Message attack_ Knowing about the message and ownership of the stego object, the aggressor attempts to uncover the embedding design.
- Chosen Stego attack_ Having possession of the stego object and the understanding of the embedding scheme, the perpetrator tries to reveal the hidden message.
- Chosen Message attack_ The assailant gathers a stego object subsequent to embedding a planned message and then tries to make sense of its relationship by cross contrasting with stego objects obtained from different messages.

## IV. A Concise Literature Review

Text based steganography is the most complicated form of information hiding [30] since a single bit change in a character code results in a different code that draws immediate attention of an onlooker or is highlighted by MS Word as a misspelled word. It falls into two categories: 1) semagrams and 2) open codes. Feature encoding of text is a trait of semagram schemes, whereas open space methods involve manipulation of white spaces between words/phrases/paragraphs/after the end of the line and alike [31]-[37]. In [38], content fragmentation of a Word 2003 file is debased, and data are inserted in the modifications which are made by the wary connoisseur. The cover degenerated file and the message all-persistent within the document permit the beneficiary to extract the hidden message based on their agreed word references. Reference [39] proposed a method for data embedding through embedding data in the chronicles of amendments, revision identifiers (RIs), made to a Word 2007 OOXML document. RIs have arbitrarily created unique values that get substituted by the scheme. Some of the earliest steganographic systems including NICETEXT [40] and Spammimic [41] generate text (stego object) upon message input.

## V. Property Coding in Microsoft Word Document for Text Steganography

In [35], authors elucidated on new text format based steganographic schemes for MS Word document. To this regard, four such methods summarized as follows:

### *A. Character Scale*

Increasing or decreasing the default text character scale, set to 100% for MS Word, displays a noticeable difference in character widths between words and spacing for the larger sized text and an overall less width difference for squeezed sizes. Noting that, the authors found 99% and 101% sized scale as insusceptible to detection. Hence, 99% sized characters to represent binary bit zero, 101% size to denote binary bit one while 100% sized characters as not contributing in bit embedding process.

For increased bit embedding capacity, it followed from above to utilize 97%-99% and 101% sizes to represent a binary bit pair that is 00, 01, 10, and 11 for each respectively, similar to the technique proposed by [3]. Resizing of words in place of characters is also doable.

### *B. Character Underline*

MS Word offers 16 different underlining styles with 224 different colors. However, for the characters underlining to get pass unnoticed, only 16 variants of white color, each representing a 4-bit unique combination, can contribute in bit hiding. Hence, each (underlined) text character serves as the holder of eight bits of the secret message. But, because characters such as *g*, *j*, *p*, *q*, and *y* undergo a noticeable change in their outlook when underlined, the same is excluded from data hiding activity.

### *C. Paragraph Borders*

The objects in MS Word such as image, text, articles can be assigned borders either as a whole or in sideways like left, right, top and bottom. Excluding the two border styles, namely, *wdLineStyleEngrave3D* and *wdLineStyleEmboss3D,* the remaining 22 are potential candidates to alias secret message bits. Any 16 amongst these styles can represent a unique quaternary bit group corresponding to the bits of the secret message.

In [30], authors used left and right borders alongside a section for data concealment using above-cited conventions. Since the quaternary bit group can represent a unique edge and also a single variant of white color at any one point of time, it follows that a total of 16 secret message bits gets embedded in conjunction with a paragraph. Because MS Word comes with 13 border styles and nine different border width, the capacity of bit stocking of the cover document gets further increased with the addition of border width.

### *D. Sentence Borders*

Given perceptibility concerns, only eight of the 16 styles of sentence bordering employed for bit embedding with only a width of 0.25 pt. A total of seven message bits get embedded in this manner with a nibble for the outside border and three bits for representing the outer edge style.

## VI. Critical Appreciation

### *A. Secrecy Assurance*

Table I illustrates the research findings of the exploration in which 127 stego objects (MS Word documents) of varying lengths, rendered by the targeted steganographic schemes automated using Microsoft® Visual Basic 6.0 Professional Edition as a tool, were analyzed against the evaluation criteria for secrecy confirmation.

### *B. On the Security of Targeted Steganographic Schemes*

Cryptography, another field of study devoted to confidentiality assurance is different from steganography, where its intent is not to hide the existence of a message but to inarticulate the secret communication by rendering it futile for the unauthorized. And the security of encryption schemes is gauged using the notion proposed in the 19th century by the Dutch cryptographer Kerckhoffs as “A cryptosystem should be secure even if everything about the system, except the key, is public knowledge” [42].

On the said analogy, it is evident that the keyless targeted steganographic schemes fall under conventional/pure steganography category which is considered weak [18]. It is so because knowing the message embedding system alone is sufficient to unhide such subsequent covert communication. Likewise, in [21], authors while elaborating on an informationtheoretic model for information security argued that the message embedding process should remain indeterministic to the attackers who also are not the case in this study.

Given the above scenario, use of the steganographic schemes discussed in this study may not get an endorsement before first strengthening its security.

### *C. Proposed Enhancements*

1) Message Embedding Steps

*a)* Convert the message along with its length into equivalent bits. Reserve two bytes for holding message length.

*b)* Select a pre-agreed 256-bit stego key and convert it into its equivalent binary. If the number of message bits exceeds 256-bit length, then:

□ *use the stego key as input to SHA-256-bit algorithm. Translate the output into equivalent binary bits. Repeat the preceding steps by appending the output bits to the other bits, until the total number of one's (binary bit 1) in resultant bits equate to or exceeds the total number of message bits plus the bits corresponding to the number representing the original message length.*

*c)* Select any MS Word file having text contents/ features ≥ number of stego bits or create a new document accordingly.

*d) Pre-processing of cover:* Iterate through the cover character by character / by paragraphs/sentence by sentence and perform random property encoding using some key dependent random number generator but within the perceptibility bounds given in Section IV.

*e)* Generate a stego key dependent random number in range 1 to ≤ (length of cover contents) which serves as the starting point for bit embedding. From this point onwards, iterate the cover contents cyclically till just before the point of departure by taking the stego key bits, in sequence, and:

*i. Check the stego key bit x ∈ {0,1}.*

*ii. If x = 0, leave the cover content at that point unattended, else apply the property coding corresponding to the secret message bit on the character/paragraph/sentence border as per the case.*

*iii. Repeat preceding two steps (i – ii) for succeeding bits till all the message bits gets embedded inside the MS Word cover file.*

2) Steps for Extracting the Hidden Message

*a)* Select the pre-agreed 256-bit stego key and convert it to its equivalent binary.

*b)* Generate a stego key dependent random number in range 1 to ≤ (length of stego object contents) which serves as the starting point for bit extraction process. From this point, onwards iterate the stego object cyclically till just before the point of departure by taking the stego key bits, in sequence, and:

*i. Check the stego key bit x ∈ {0,1}.*

*ii. If x = 0, leave the cover content at that point unattended, else interpret the property coding corresponding to that bit as either zero or one as per the case.*

*iii. Repeat preceding two steps for succeeding bits till the first sixteen hidden bits gets extracted. Convert these into corresponding decimal value. The result is the number of hidden message bits.*

*iv. If the number of hidden bits exceeds 256-bit length, then:* □ use the stego key as input to SHA-256-bit algorithm. Translate the output into equivalent binary bits. Repeat the preceding steps by appending the output bits to the other bits, until the total number of one's (that is, binary bit 1) of resultant bits equate to or exceeds the total number of hidden bits.

*v. Repeat steps (i to ii) for till extraction of all the hidden message bits is complete.*

*c)* Convert the extracted bits into corresponding character codes. The result of the concatenation of such characters is the secret message.

### *D. Signifying Proposed Enhancement*

1) Steganographic Procedure of Targeted Schemes*:*

The equations for message bit embedding and extraction are as shown below:

$$\textit{Message Embedding: Stego.Object} \leftarrow \partial\ (M,C) \qquad (1)$$

$$\textit{Message Extraction:}\quad M' \leftarrow \tilde{\alpha}\ (\textit{Stego.Object}) \qquad (2)$$

$$(1)\&(2) \Rightarrow M' \leftarrow \tilde{\alpha}\ (\textit{Stego.Object}) \leftarrow \partial\ (M,C) \qquad (3)$$

$$M' = M \qquad (4)$$

where M = message bits – just before embedding, M' = message bits – after bits' extraction, C = MS Word Document, $\partial$ = bit embedding process, and $\tilde{\alpha}$ = bit extraction process. Moreover, the schemes do not offer any resistance against the known cover or any other type of attacks.

2) Steganographic Procedure of Proposed Schemes

The equations for message bit embedding and extraction are as:

$$\textit{Pre-processing of Cover:}\ \varepsilon \leftarrow \partial\ (\textit{cover}, \acute{K}_1) \qquad (5)$$

$$\textit{Message Embeding: Steg.Object} \leftarrow \ddot{\partial}\ (M, \acute{K}_2, \varepsilon) \qquad (6)$$

$$\textit{Message Extraction: } M' \leftarrow \tilde{\alpha}\ (\textit{Stego.Object}) \qquad (7)$$

$$(6)\&(7) \Rightarrow M' \leftarrow \tilde{\alpha}\ (\textit{Stego.Object}) \leftarrow \ddot{\partial}\ (M, \acute{K}_2, \varepsilon) \qquad (8)$$

$$\textit{from (1)}, M' = \leftarrow \ddot{\partial}\ (M, \acute{K}_2, \partial\ (\textit{cover}, \acute{K}_1)) \qquad (9)$$

where $\partial$ denotes pre-processing function, $\acute{K}_1$ is the random key for pre-processing, $\acute{K}_2$ is the stego key, $\ddot{o}$ is the bit embedding process, and $\tilde{o}$ is the bit extraction process

It follows from above that without the knowledge of $K_2$ & $K_1$, a malicious attacker cannot arrive on the hidden message by launching any of the known attacks, thereby ensuring the security of the targeted systems proposed for stealth communication.

### *E. Way Forward*

For increased capacity, the recommendation is to compress the message before its encryption.

## VII. Conclusion

This paper attempts to analyze the security of some of the information hiding schemes that exploit the flexibility of certain property attributes of Microsoft Word document. The scenario deliberated assumes two parties engaged in stealth exchange of messages in the presence of passive surveillance by the evil invader. Evidence-based limitations of such steganographic schemes in providing security cover to hidden communication demonstrated followed by a proposition to their security augmentation justified through mathematical annotation. The implicit finding of this study elucidates that in today's High-Tec immersive computing environment, steganographic schemes evolved must take into consideration the security aspect of information whether it is at rest (persistent storage) or in transit.

## References


[1] Dretske, Fred. "Knowledge and the Flow of Information." (1981).

[2] Pfitzmann, B., "Information Hiding Terminology," Proc. of First Internet Workshop on Information Hiding, Cambridge, UK, 1996, pp. 347-350.

[3] Rafat, K. F., "Digital Steganography For Ascii Text Document" Ph.D. dissertation, Dept. Comp. Science., International Islamic University, Islamabad, 2014.

[4] Petitcolas, F. A. P.; Anderson, R. J.; Kuhn, M. G.: Information hiding survey. In: Proceedings of the IEEE, Special Issue on Protection of Multimedia Content, vol. 87, no. 5, pp. 1062–1078 (1999).

[5] Artz, Donovan. "Digital steganography: hiding data within data." IEEE Internet Computing 5, no. 3 (2001): 75-80.

[6] Djebbar, Fatiha, Beghdad Ayad, Karim Abed Meraim, and Habib Hamam. "Comparative study of digital audio steganography techniques." EURASIP Journal on Audio, Speech, and Music Processing 2012, no. 1 (2012): 1-16.

[7] McClaskey, Carolyn Marie. "Factors affecting relative pitch perception." (2016).

[8] Georgiev, Mihail, and Atanas Gotchev. "Method and Apparatus For Downscaling Depth Data For View Plus Depth Data Compression." U.S. Patent 20,160,094,829, issued March 31, 2016.

[9] Valentín, Kristián, Peter Wild, Svorad Štolc, Franz Daubner, and Markus Clabian. "Optical benchmarking of security document readers for automated border control." In SPIE Security+ Defence, pp. 999502999502. International Society for Optics and Photonics, 2016.

[10] Gupta, Richa, and Priti Sehgal. "A survey of attacks on iris biometric systems." International Journal of Biometrics 8, no. 2 (2016): 145-178.

[11] Ivančević, Tajana Koren, Maja Rudolf, and Nikolina Stanić Loknar. "Steganography of vector graphics and typography in infrared security printing." Acta Graphica 27, no. 1 (2016).

[12] Petitcolas, Fabien AP, Ross J. Anderson, and Markus G. Kuhn. "Information hiding-a survey." Proceedings of the IEEE 87, no. 7 (1999): 1062-1078.

[13] Arnold, Michael, Martin Schmucker, and Stephen D. Wolthusen. Techniques and applications of digital watermarking and content protection. Artech House, 2002.

[14] Johnson, Neil F., Zoran Duric, Sushil Jajodia, and Nasir Memon. "Information hiding: steganography and watermarking—attacks and countermeasures." Journal of Electronic Imaging 10, no. 3 (2001): 825826.

[15] Kahn, D. Codebreakers: The Story of Secret Writing. Revised ed., Scribner, New York, 1996.

[16] Wayner, Peter. Disappearing Cryptography: information hiding: steganography & watermarking. Morgan Kaufmann, 2009.

[17] Pfitzmann, B.: Information hiding terminology. In: Anderson, R. (ed.) Information Hiding, 1st International Workshop, vol. 1174 of Lecture Notes in Computer Science, pp. 347–350. Springer (1996).

[18] Dunbar, Bret. "A detailed look at Steganographic Techniques and their use in an Open-Systems Environment." Sans Institute 2002 (2002): 1-9.

[19] G. J. Simmons, "The prisoners' problem and the subliminal channel." in Advances in Cryptology: Proceedings of Crypto 83 (D. Chaum, ed.), Plenum Press, 1984, pp. 51–67.

[20] Dourish, Paul, Rebecca E. Grinter, Jessica Delgado De La Flor, and Melissa Joseph. "Security in the wild: user strategies for managing security as an everyday, practical problem." Personal and Ubiquitous Computing 8, no. 6 (2004): 391-401.

[21] J. Zöllner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, G. Wicke, G. Wolf. "Modeling the security of steganographic systems." Proc. 2nd Workshop on Information Hiding, April 1998, Portland, LNCS 1525, Springer-Verlag, 1998, pp. 345-355.

[22] Gregory Kipper. Investigator's Guide to Steganography. Auerbach Publications, October 2003, pp. 240.

[23] Johnson, Neil F., and Sushil Jajodia. "Exploring Steganography: Seeing the unseen." Computer 31, no. 2 (1998): 26-34.

[24] Ali Al-Ataby and Fawzi Al-Naima. "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform." The International Arab Journal of Information Technology, Vol. 7, No. 4, pp. 358-364, October 2010.

[25] Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett. "Steganography and digital watermarking." Internet:http://www.cs.bham.ac.uk/~mdr/teaching/modules03 /security/st udents/SS5/Steganography.pdf (Last Accessed on September 5, 2016).

[26] Debnath, Bikash, Jadav Chandra Das, Debashis De, and Timam Ghosh. "Image masking using quantum-dot cellular automata." In Devices, Circuits and Systems (ICDCS), 2016 3rd International Conference on, pp. 231-235. IEEE, 2016.

[27] Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi. "A Survey on Image Steganography and Steganalysis." Journal of Information

Hiding and Multimedia Signal Processing,Vol. 2, April 2011, pp. 142-172.
[28] Provos, Niels, and Peter Honeyman. "Hide and seek: An introduction to steganography." IEEE Security & Privacy 1, no. 3 (2003): 32-44.
[29] A. Westfeld and A. Pfitzmann. “Attacks on steganographic systems,” in
Proc. 3rd Int. Workshop on Information Hiding, 1999, vol. 1768, pp.61– 76.
[30] 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.
[31] Bender, Walter, Daniel Gruhl, Norishige Morimoto, and Anthony Lu. "Techniques for data hiding." IBM systems journal 35, no. 3.4 (1996): 313-336.
[32] Por, L. Y., and B. Delina. "Information hiding: A new approach in text steganography." In WSEAS International Conference. Proceedings. Mathematics and Computers in Science and Engineering, edited by Qing Li, S. Y. Chen, and Anping Xu, no. 7. World Scientific and Engineering Academy and Society, 2008.
[33] Por, Lip Yee, KokSheik Wong, and Kok Onn Chee. "UniSpaCh: A textbased data hiding method using Unicode space characters." Journal of Systems and Software 85, no. 5 (2012): 1075-1082.
[34] Khairullah, M. D. "A novel text steganography system using font color of the invisible characters in Microsoft Word documents." In Computer and Electrical Engineering, 2009. ICCEE'09. Second International Conference on, vol. 1, pp. 482-484. IEEE, 2009.
[35] Stojanov, Ivan, Aleksandra Mileva, and Igor Stojanovic. "A New Property Coding in Text Steganography of Microsoft Word Documents." (2014): 25-30.
[36] Khadim, Umair, Aihab Khan, Basheer Ahmad, and Ahmed Khan. "Information Hiding in Text to Improve Performance for Word Document." International Journal of Technology and Research 3, no. 3 (2015): 50.
[37] Xiang, Lingyun, Caixia Sun, Niandong Liao, and Weizheng Wang. "A Characteristic-Preserving Steganographic Method Based on Revision Identifiers." International Journal of Multimedia and Ubiquitous Engineering 11, no. 9 (2016): 29-38.
[38] Liu, Tsung-Yuan, and Wen-Hsiang Tsai. "A new steganographic method for data hiding in Microsoft Word documents by a change tracking technique." IEEE Transactions on Information Forensics and Security 2, no. 1 (2007): 24-30.
[39] Z. Fu, X. Sun, J. Zhang, and B. Li, “A novel watermark embedding and detection scheme based on zero- knowledge proof,” International Journal of Digital Content Technology and Its Applications, vol. 5, no. 3, pp. 273–286, 2011.
[40] M. Chapman, “NICETEXT,” 2014, ftp://www.zedz.net/pub/security/steganography/nicetext/. Accessed on Nov.10, 2017.
[41] Spammimic, February 2014, http://www.spammimic.com. Accessed on Nov.10,2017
[42] Petitcolas, Fabien AP. "Kerckhoffs’ principle." In Encyclopedia of cryptography and security, pp. 675-675. Springer US, 2011.