ISSN (O) 2321-2004, ISSN (P) 2321-5526

IJIREEICE

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 12, December 2021

DOI: 10.17148/IJIREEICE.2021.91205

High security object integrity and manipulation of conceal information by hiding partition technique

GIRISH PADHAN

Associate professor, Electrical Electronics Engineering, Vikash institute of technology, Bargarh, Indian

Abstract: In the current period, because of the far reaching accessibility of the Internet, it is incredibly simple for individuals to convey and share interactive media substance with one another. Nonetheless, simultaneously, secure exchange of individual and protected material has turned into a basic issue. Thusly, secure method for information move are the most dire need of the time. Steganography is the science and specialty of shielding the restricted information from an unapproved access. The steganographic approaches hide restricted information into a cover record of type sound, video, text or potentially image. The genuine test in steganography is to accomplish high strength and limit without dealing on the subtlety of the cover document. In this article, a proficient steganography strategy is proposed for the exchange of privileged information in computerized images utilizing number hypothesis. For this reason, the proposed technique addresses the cover image utilizing the Fibonacci grouping. The portrayal of an image in the Fibonacci succession permits expanding the bit planes from 8-bit to 12-bit planes. The test aftereffects of the proposed strategy in examination with other existing steganographic strategies display that our technique accomplishes high installing of privileged information as well as gives top caliber of stego images as far as pinnacle signal-to-clamor proportion (PSNR). Besides, the power of the technique is likewise assessed within the sight of salt and pepper clamor assault on the cover images.

Keywords: Security, Object , Integrity , Manipulation , Information , Hiding, Partition ,Technique

I. INTRODUCTION

Presently a day's normal correspondence of information transmission is done effectively by online media like images, recordings, and sounds for digital correspondence. Sharing, stockpiling, business, eservices like aircraft reservations, Internet business, media communications charging, electronic banking, exchange preparing, Visas, capital stock exchanging, life sciences research, medical care claims handling, and a lot more exercises are acted in our everyday existence schedule. Expanding conditions of digital correspondence force a few difficulties in ensuring and overseeing information as gotten correspondence. Altering becomes simpler because of effectively accessible programming. A significant proportion of confirmation assortment, stockpiling, and verification in criminological sciences, which chooses the wellbeing and security of any framework records, can be either in versatile archive organizes or filtered images. To accumulate proof, or plan a measurable examination, digital images are gotten with various present day strategies. Information hiding, achieved by taking advantage of a PC's record framework and different other working framework qualities, can take on many structures. Much of the time, information hiding is a purposeful movement that an individual utilizes to store away touchy information trying to make it imperceptible to every other person. Notwithstanding, there are a few special cases, for example, digital watermarking, that are utilized for fitting purposes. Some normal techniques for information hiding include: stowed away documents, erased records, stowed away partitions, substitute information streams, steganography, and slack space hiding. There are numerous PC criminology toolboxs accessible that permit a client to recognize different sorts of information hiding.

Taking a more top to bottom look to how these tool stash identify the kinds of information hiding referenced gives a more profound comprehension of how the information hiding was cultivated. The most generally utilized document frameworks for Windows working frameworks are the record allotment table (FAT) record frameworks and the new advances document framework (NTFS). These record frameworks both play out similar fundamental errands, yet for the motivations behind information hiding, their unpretentious contrasts change the manners in which that a few techniques for information hiding are refined. In this manner, a short outline of each document framework, alongside a little conversation of their disparities is justified and will be introduced preceding the conversation of the different techniques for information hiding. Digital image investigation incorporates image recuperation and reconnaissance for image information improvement. The objective of fraud location is to amplify the extraction of information from controlled images, especially uproarious and post- handled images. Since digital image preparing is becoming famous with many benefits in logical and designing applications, the imitation techniques are likewise developing at a quick rate. In any case, the validness of images and recordings becomes shifty information as addressed by Garfinkel in Digital image scientific methodologies beat image altering and expect to further develop image quality for the present digital world by

ISSN (O) 2321-2004, ISSN (P) 2321-5526

IJIREEICE

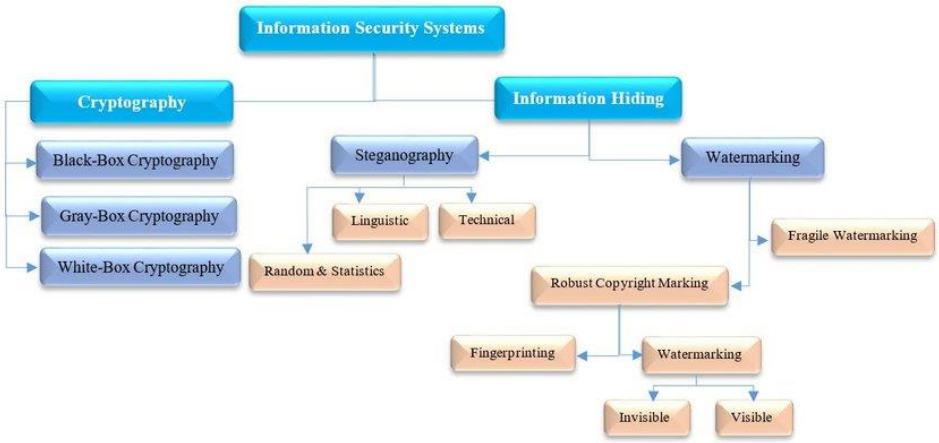
International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 12, December 2021

DOI: 10.17148/IJIREEICE.2021.91205

featuring the requirement for new strategies for creativity and its quality. Information on the image input source is significant since it permits gadget information for agents' necessities. The most well-known sort of duplicate move altering was generally used in a digital exchange where a piece or some segment of an image messed with comparable provisions of a similar image, and that made it hard to gauge the exactarea of the image imitations.

The different categories of information security systems are depicted in Figure 1. The cryptography and information hiding are security systems that are used to protect data from deceivers, crackers, hackers, and spies. Commonly, most of the malicious users want to leave traces from cuts, manipulations, and infections [7]. The cryptography scrambles a plain text into ciphertext which is reversible without data loss. The goal of cryptography is to prevent unauthorized access to the secret information by scrambling the content of information. On the other hand, information hiding is a powerful security technique which hides a secret data in a cover media (e.g., text, image, audio, or video) so that the trace of embedding hidden data is completely unnoticeable. The cryptography and information hiding are similar in a way that both are utilized to protect sensitive information. However, the imperceptibility is the difference between both techniques; that is, information hiding concerns how to hide information unnoticeably. Generally, the information hiding can be further categorized into steganography and watermarking. The aim of steganography is to hide a secret message in a cover media in order to transmit the secret information; therefore, the main concern is how to conceal the secret information without raising suspicion; that is, steganography needs to conceal the fact that the message is hidden. Watermarking is concerned with hiding a small data in digital files such that the hidden data is robust to alterations and adjustments. In other words, watermarking aims to protect intellectual property of digital media against unauthorized copy or access by embedding a watermark (visible or invisible) in the cove media which can remain beside the data, and it can be used whenever there is any query about the originality of media (e.g., the hidden watermark refers to the original owner) [2–10].



The image size of altered areas is likewise a significant boundary for the recognition offalsification. At the point when post-handling is applied then the outcome will be an inferior quality factor that will make calculations troublesome. Digital legal is an assortment of logical strategies for distinguishing proof, investigation, understanding, content validation, characterization, documentation from digital hotspots for the reproduction of unique information, which helps in fraud location in this manner recognizing who, what and why in such conditions. Measurable science is vital for image examination in which factual twofold examples were investigated utilizing distinctive change techniques.

II. LITERATURE REVIEW

In what follows, we describe the existing literature on text watermarking including architecture, the Unicode standard, text watermarking categories, applications, evaluation criteria, and attacks.

2.1. Text Watermarking Architecture

As shown in Figure 2, digital text watermarking includes two main phases, namely, watermark embedding and watermark extraction.

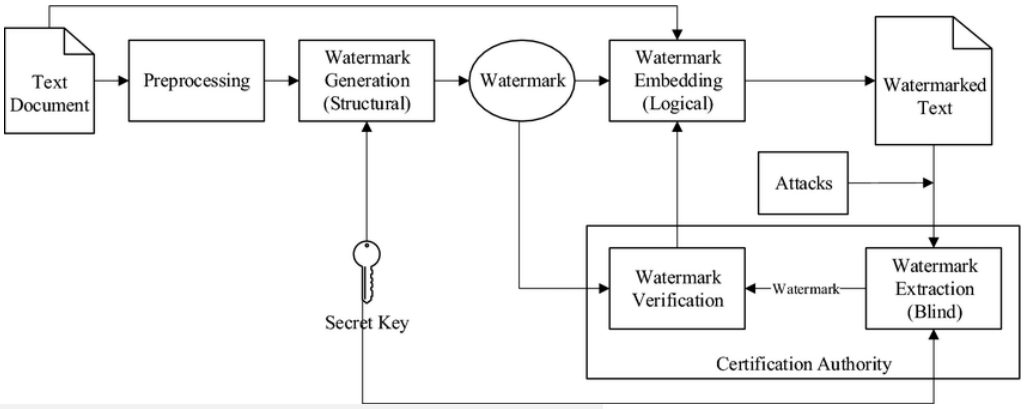
ISSN (O) 2321-2004, ISSN (P) 2321-5526

IJIREEICE

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 12, December 2021

DOI: 10.17148/IJIREEICE.2021.91205



(Digital text watermarking (embedding and extraction) architecture.)

Watermark Embedding. The embedding phase of text watermarking algorithm includes three stages. The first stage is generating a watermark string which includes the owner's name or other pieces of information (e.g., author and publisher). In the second stage, the watermark string is converted to a binary string, which is modified by a hash function according to an optional key, and then an invisible watermark string is generated for embedding it into special locations in the cover text. Finally, it is inserted into special locations where the watermark string will not be affected by attacks.

2.2. Unicode Standard

In the digital text processing system, the Unicode standard to process and display digital texts from 1987 until now has been defined. Basically, all operating systems and writing software systems have to support the Unicode standard for representation of digital texts. The Unicode standard is a universal character encoding system designed to support the worldwide display, processing, and interchange of the texts with different languages and technical disciplines. In addition, it also supports the historical and classical letters in many languages. This standard is compatible with the latest version of ISO/IEC 10646-1:2017 and has the same characters and codes of ISO/IEC 10646. As of June 2017, the latest version of Unicode is 10.0.0 is maintained by the Unicode Consortium. It includes three encoding forms such as UTF-8, UTF-16, and UTF-32 which the Unicode allows for 17 planes, each of 65,536 possible characters (or "code points"). This gives a total of 1,114,112 possible characters in different formats such as digits, letters, symbols, and a huge number of current characters in various languages around the world. Currently, the most commonly used encoding forms are UTF-8, UTF-16, and now-outdated UCS-2. UTF-8 provides one byte for any ASCII character.

2.3. Text Watermarking Categories

During past two decades, many types of research have been carried out based on structural (format based), linguistic, scanned-image watermarking and frequency of words in the cover text. Herein, we consider those methods which are focused on modifying the structure and content of the cover text. In case of text processing, watermarking techniques are divided into two main categories, linguistic and structural. The linguistic technique concerns with the special features of the text content that can be changed in a specific language, and moreover, the structural technique concerns with the layout or format of the cover text that can be modified [6, 18], although some researchers have classified the text watermarking techniques based on the features of methods such as robust, fragile, invisible, and visible.

EC= BPL* Total location

(ii) Embedding Capacity (EC). The number of watermark bits which can be concealed in a cover text is termed as embedding capacity. This criterion can be measured numerically in units of bit-per-locations (BPL). Location means a specific position in the cover text where the algorithm can embed the watermark string (e.g., spaces between words and after special punctuations). Even though a watermarking algorithm provides a large embedding capacity, it is not desirable for copyright protection, if it alters the cover text profoundly.

Steganography is in the (particularly military) writing likewise alluded to as transmission security. Steganographic technique tracks down its fundamental application in the field of mystery correspondence. It very well may be utilized by insight organizations across the world to trade profoundly classified information in a secret way for example a spy can conceal a guide of a psychological militant camp in a photo utilizing image steganographic programming and post it on a public conversation board or discussion. An official from the administrative center could download the photo from the discussion and effectively recuperate the secret guide. Steganographic techniques can likewise forestall an authentic element against intimidation for example on the off chance that proprietary advantages are encoded and put away on hard plates they can be effectively noticeable and a pernicious client might force the genuine client to unveil something similar. Digital portrayal of signs brings many benefits when contrasted with simple portrayals, like lossless recording and replicating, advantageous dispersion over networks, simple altering and alteration, and sturdy, less expensive,

ISSN (O) 2321-2004, ISSN (P) 2321-5526

IJIREEICE

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 12, December 2021

DOI: 10.17148/IJIREEICE.2021.91205

effectively reachable documented. Shockingly, these benefits additionally present major issues including wide spread copyright infringement, unlawful duplicating and dissemination, dangerous confirmation, and simple manufacturing. Robbery of digital photos is as of now a typical marvel on the Internet. Today, digital photos or recordings can't be utilized in the chain of care as proof in the court as a result of nonexistence of a dependable system for confirming digital images or alter location. Information hiding in digital archives gives a way to conquering those issues.

III. REQUIREMENTS OF HIDING INFORMATION DIGITALLY

There are various conventions and inserting techniques that empower us to shroud information in a given object. In any case, the entirety of the conventions and techniques should fulfill various necessities so steganography can be applied accurately.

Coming up next is a rundown of primary necessities that steganography techniques should fulfill: The integrity of the secret information after it has been implanted inside the stego object should be right.

1. The secret message should not change at all, for example, extra information being added, loss of information or changes to the privileged data after it has been covered up. In the event that restricted intel is changed during steganography, it would nullify the entire purpose of the cycle.
2. The stego object should stay unaltered or almost unaltered to the unaided eye. In the event that the stego object changes fundamentally and can be seen, an outsider might see that information is being covered up and subsequently could endeavor to extricate or to obliterate it.
3. In watermarking, changes in the stego object must have no impact on the watermark. Suppose you had an unlawful duplicate of an image that you might want to control differently.
4. These manipulations can be straightforward cycles, for example, resizing, managing or pivoting the image. The watermark inside the image should endure these manipulations, in any case the assailants can without much of a stretch eliminate the watermark and the place of steganography will be broken.
5. Finally, we generally accept that the aggressor knows that there is covered up information inside the stego object.

Digital Image Forensic Techniques for Feature Extraction

Change is vital in a few image preparing applications like Image examination, Image separating, Image upgrade, and Image pressure. Change having sinusoidal as the essential capacity is called Fourier Transform. Change having nonsinusoidal as an essential capacity is called Haar-Transform (most straightforward), Walsh Transform, Hadamard-Transform, and inclination Transform. Change whose essential cycle relies upon measurements of the info signal is KL Transform (best direct Transform as far
energy compaction) and Singular Value Decomposition. Change which addresses directional information of an image signal incorporates Hough Transform, Radon change.

Spatial Transform Techniques

This methodology extricates highlights dependent on Scale Invariant Feature Transform and Speed up Reduced Features, second, power, obscure, Zernike approach, and so forth

Training and Testing Procedure of Passive Forgery Detection Techniques This incorporates the course of Image Processing and Feature Extraction wherein highlights from a specific set are taken out for each class which helps in distinctive that from additional classes while staying invariant to recognizing modifications inside the class from input counterfeit information. Extricated edifying elements and picked highlights should be unpretentious to image manipulation and low measurement diminishes the computational multifaceted nature of grouping and preparing without decreasing AI execution. Classifier Selection helps the classifier in separating highlights from preparing image sets and Feature Pre Processing Classification and post-handling is associated with manufactured district examination.

Digital images are prepared and tried with MICC-220 datasets and ongoing datasets. In this preparation method, image datasets incorporate unique and altered images. In the assessment cycle, 100 images are taken for preparing and testing systems.

IV. CONCLUSION

Duplicate moving falsification recognition has been tried by numerous systems for the extraction of components, division, procurement, histogram, change, and so forth Subsequently, the confirmation of digital images is a vital region in the field of scientific examination on image preparing. This examination assists with distinguishing new approaches and thoughts for future specialists working in the field of electronic fraud recognizable proof. Duplicate moving phony discovery calculation is executed with all image limitations and works with no speculated image subtleties like a digital watermark or digital mark.

ISSN (O) 2321-2004, ISSN (P) 2321-5526

IJIREEICE

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 12, December 2021

DOI: 10.17148/IJIREEICE.2021.91205

REFERENCES

[1]. [1] Y.Q Shi, XL, X. Zhang, H.-T. Wu and B. Ma, "Reversible data hiding Advances in the past two decades", IEEE Access, vol. 4. pp. 3210-3237, 2016
[2]. [2] J. Fridrich, M. Goljan and R Du, "Invertible authentication". Proc SPIE Secur Watermarking Multimedia Contents III, vol. 4314, pp. 197-208. Aug 2001
[3]. [3] J Fridrich, M. Goljan and R. Du "Lossless data embedding New paradigm in digital watermarking" EURASIP J. Adv Signal Process., vol. 2002, Dec. 2002
[4]. [4] M.U. Celik, G. Sharma, A M Tekalp and E Saber, "Lossless generalized-LSB data embedding", IEEE Trans. Image Process, vol. 14, no. 2, pp 253-266. Feb. 2005.
[5]. [5] J. Tian, "Reversible data embedding using a difference expansion", IEEE Trans Circuits Syst Video Technol, vol. 13, no. 8, pp. 890-896, Aug 2003 → Show in Context View Article Full Text PDF (544KB) Google Scholar
[6]. [6] J. Tian, "Wavelet-based reversible watermarking for authentication". Proc. SPIE Secur Watermarking Multimedia Contents IV, vol 4675, pp. 679-690 Apr 2002
[7]. [7] Mayer, O. and Stamm, M. C."Forensic Similarity for Digital Images", IEEE
[8]. Transactions on Information Forensics and Security, vol 3456 15(1), pp. 1331–1346.
[9]. Jun.2017
[10]. [8] Matern, F., Riess, C. and Stamminger, M. "Gradient-Based Illumination Description for Image Forgery Detection", IEEE Transactions on Information Forensics and Security. IEEE, vo.2341, pp. 1303–1317. Apr 2020
[11]. [9] Ryu, S. et al. "Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments", IEEE Trans. Information Forensics and Security, vol. 762 pp. 1355–1370.jan 2018
[12]. [10] Joshi, S., Member, S. and Khanna, N. "Single Classifier-based Passive System for Source Printer Classification using Local Texture Features", IEEE Trans.
[13]. Information Forensics and Security, vol. 4217 pp. 1603–1614. Mar 2019
[14]. [11] Tang, C., Kong, A. W. K. and Craft, N. "Using a knowledge-based approach to remove blocking artifacts in skin images for forensic analysis", IEEE Transactions on Information Forensics and Security, vol.3421 pp. 1038–1049. Mar 2018
[15]. [12] Fan, W. et al. " JPEG anti-forensics with improved trade off between forensic undetectability and image quality", IEEE Transactions on Information Forensics and Security, vol 4321 pp. 1211–1226. May 2018
[16]. [13] Y. M. Alginahi, M. N. Kabir, and O. Tayan, "An enhanced Kashida-based watermarking approach for Arabic text-documents," in *Proceedings of the 2013 10th International Conference on Electronics, Computer and Computation, ICECCO 2013*, pp. 301–304, Turkey, November 2013.View at: Publisher Site | Google Scholar
[17]. [14] Y. M. Alginahi, M. N. Kabir, and O. Tayan, "An enhanced kashida-based watermarking approach for increased protection in arabic text-documents based on frequency recurrence of characters," *International Journal of Computer and Electrical Engineering*, vol. 6, no. 5, pp. 381–392, 2014.View at: Publisher Site | Google Scholar
[18]. [15] L. Y. Por, K. Wong, and K. O. Chee, "UniSpaCh: A text-based data hiding method using Unicode space characters," *The Journal of Systems and Software*, vol. 85, no. 5, pp. 1075–1082, 2012.View at: Publisher Site | Google Scholar
[19]. [16] M. Dalla Preda and M. Pasqua, "Software watermarking: a semantics-based approach," *Electronic Notes in Theoretical Computer Science*, vol. 331, pp. 71–85, 2017.View at: Publisher Site | Google Scholar
[20]. [17] J. Gu and Y. Cheng, "A Watermarking scheme for natural language documents," in *Proceedings of the 2010 2nd IEEE International Conference on Information Management and Engineering, ICIME 2010*, pp. 461–464, China, April 2010.View at: Publisher Site | Google Scholar
[21]. [18] R. J. Jaiswal and N. N. Patil, "Implementation of a new technique for web document protection using unicode," in *Proceedings of the 2013 International Conference on Information Communication and Embedded Systems, ICICES 2013*, pp. 69–72, India, February 2013.View at: Publisher Site | Google Scholar
[22]. [19] T.-Y. Liu and W.-H. Tsai, "A new steganographic method for data hiding in microsoft word documents by a change tracking technique," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 1, pp. 24–30, 2007.View at: Publisher Site | Google Scholar
[23]. [20] A. A. Mohamed, "An improved algorithm for information hiding based on features of Arabic text: A Unicode approach," *Egyptian Informatics Journal*, vol. 15, no. 2, pp. 79–87, 2014.View at: Publisher Site | Google Scholar
[24]. [21] N. A. Salem Al-maweri, W. A. Wan Adnan, A. R. Ramli, K. Samsudin, and S. M. Ahmad Abdul Rahman, "Robust Digital Text Watermarking Algorithm based on Unicode Extended Characters," *Indian Journal of Science and Technology*, vol. 9, no. 48, pp. 1–14, 2016.View at: Google Scholar
[25]. [22] S. G. Rizzo, F. Bertini, and D. Montesi, "Content-preserving Text Watermarking through Unicode Homoglyph Substitution," in *Proceedings of the 20th International Database Engineering & Applications Symposium (IDEAS '16)*, pp. 97–104, 2016.View at: Google Scholar
[26]. [23] Y. Zhang, H. Qin, and T. Kong, "A novel robust text watermarking for word document," in *Proceedings of the 3rd International Congress on Image and Signal Processing (CISP '10)*, pp. 38–42, October 2010.View at: Publisher Site | Google Scholar
[27]. [24] H. O. N. Hebah, "Digital watermarking a technology overview," *International Journal of Research and Reviews in Applied Sciences*, vol. 6, no. 1, pp. 98–102, 2011.View at: Google Scholar
[28]. [25]J.Klensin,"UnicodeControlcharacters,Fileformate,"2017, http://www.fileformat.info/info/unicode/char/search.htm.View at: Publisher Site | Google Scholar

BIOGRAPHY

Dr Girish padhan,a young lad of 38 years from a weleducated rural family,working as a associate professor in VIT,Bargarh odisha having a dozen of national and international papers go ahead on the area of image processing.