International Journal of Engineering& Scientific Research
Vol.10 Issue 02, February 2022
ISSN: 2347-6532 Impact Factor: 6.660
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

AN EMBEDD STEGANOGRAPHIC TECHNIQUES AND WATERMARKING FOR DIGITAL IMAGES

ANJALI CHATURE
Assistant Professor
Dept. of Electronics and Communication Engineering
Government Engineering College
Chamarajanagara, Karnataka, India.

***Abstract*—** The development of information technology has led to a dramatic increase in the distribution of multimedia traffic to data networks. This has necessitated the resolution of the following information protection functions for multimedia data: protection against the leaking of confidential information, and the identification of a leak source; to ensure the impossibility of unauthorized changes; copyright protection of digital objects. To solve this type of problem, steganography and watermarking techniques are designed to use digital embedding and sequence of hidden information for a variety of purposes. In this paper, a promising research is provided in a particular area. It provides basic information about this field of research and considers the main uses of its methods. Displays current trends in the development of data encryption methods and algorithms for digital images. It focuses on current activities that reflect current research guidelines in the field of digital embedding in digital photography.

Keywords— Digital image Steganography, Information security, Digital watermarking.

I. INTRODUCTION

In today's world, the importance of protecting digital data is extremely high. One of the ways to ensure the security of digital data is to use steganography and digital marking methods. This is especially important for multimedia data, such as photos, audio recordings, video files. Hiding information with the help of steganography and digital watermark embedding is an established and evolving science field.

The development of information technology has led to a dramatic increase in the distribution of multimedia traffic to data networks. This has necessitated the resolution of the following information protection functions for multimedia data: protection against the leaking of confidential information, and the identification of a leak source; to ensure the impossibility of unauthorized changes; copyright protection of digital objects. To solve this type of problem, steganography and watermarking techniques are designed to use digital embedding and sequence of hidden information for a variety of purposes.

Steganography includes the protection of some additional information embedded in the digital cover object. The information itself, as well as the cover we are hiding, can be a variety of things in themselves. The main idea of stenographic methods is to make embedded information invisible to the attacker. Thanks to this statement, confidential information can be transmitted securely via an open communication channel, as only the sender and receiver will be able to have its presence within the transferred cover.

Digital watermark methods are used for the important protection of the digital cover itself. The functions of the digital watermark are the same as those of the digital signature functions. A digital watermark is a label that allows to identify the author of a digital object, or to verify the authenticity and integrity of an object. Digital watermarks are often used to protect the identity of multimedia files, to control data integrity, and to verify sources of this data. An old digital watermark app connected to multimedia protection. For now, however, the use of such data protection methods of various kinds is warranted. It therefore creates the need to address data protection functions in order to provide protection from multimedia data leaks.

II. LITERATURE SURVEY

In [1], the steganographic embedding algorithm for information in coloured pictures is displayed. Embedding using the LSB method was performed on the coefficients of the DCT. In this case, the RGB image plane is pre-processed for selection random pixels will be used for embedding. Randomly the selection of pixels protects the algorithm from malicious attacks and resists benchmark steganalysis tools. AGA is used to increase the durability and invisibility of embedding.

In paper [2] suggests a hybrid watermark algorithm embedding. The watermark is placed in the centre of the DCT DFT size band. The authors argue that the combination of the two variables increases the ambiguity in the use of DFT and increases durability due to use of the DCT. Prior to embedding, the watermark is encrypted and during embedding, a watermark the pieces are replaced

The authors of [3] propose their steganography approach of data hidden in key bits' pixels. Embedding occurs in two stages. In the first phase, 2 bits' details embedded in each image pixel, too two converted pixels combined into a medium pair pixel. In the second stage, a pair of intermediate is used Pixels, two different identical pairs are found to hide the other secret pieces, because it is possible to achieve great embedding capacity.

In [4] an algorithm of deferred was introduced steganographic embedding information in JPEG compressed images, which differ in the original method of selection of the coefficients of the DCT, the variation of which leads to less distortion of the cover image during embedding. Verification conversions, message lengths and coefficients used to embed message hidden inside an image and the message itself.

The authors of [5] suggest an embedded method based on MSB predictions. Inside the framework of this approach, two

International Journal of Engineering& Scientific Research
Vol.10 Issue 02, February 2022
ISSN: 2347-6532 Impact Factor: 6.660
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

different approaches explained. The first of them, a high volume backwards to hide data by fixing predictive errors, does not allow you to completely restore the original data, however has high volume, and the restored image is very close in the first. Second, high renewable capacity to hide data with embedded prediction errors, has a slightly lower capacity due to the built-in location map, but it has a full setback.

In [6], IWT is used for this. Local maps produced according to the most important small aircraft of high coefficients. Additional location maps un-mountable compression and, along with confidential data, are available embedded in very important high-frequency bits' wavelet coefficients for changing bits. In this case, the real thing the image can be fully restored only if both encrypted key and embedding key known. Only have encryption key, you can access the image, but it will contain data embedded and will not be the same as the original. Use of IWT is defined by the absence of information loss.

III. DIGITAL STEGANOGRAPHY

Steganography is a way of storing information by concealing that information. It can be used to perform secret transactions and thus improve individual privacy. Steganography aims to communicate confidential data with the appropriate multimedia carrier. It is the custom to hide a secret message after a normal message. It comes from two Greek words, "steganos", meaning cover and "graphia", meaning to write. Steganography is an ancient tradition, practiced in various ways for thousands of years to keep communication a secret. For example: The first use of steganography can be traced back to 440 BC when in ancient Greece, people wrote messages on wood and covered it with wax, which served as a cover. The Romans used various types of Invisible Ink, to convey the hidden messages by means of light or heat. During World War II the Germans brought small dots, which were complete texts, photographs, and plans cut down to a dot and pasted on regular paper. Null Ciphers are also used to hide unsolicited private messages in a standard message that looks innocent.

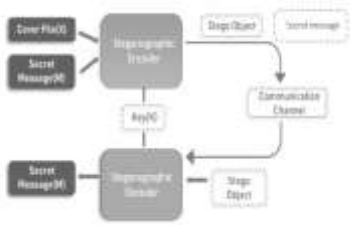

Figure 1: Steganography Process

As the image depicts, both cover file(X) and secret message(M) are fed into steganographic encoder as input. Steganographic Encoder function, f(X,M,K) embeds the secret message into a cover file. Resulting Stego object looks very similar to your cover file, with no visible changes. This completes encoding. To retrieve the secret message, Steganographic Object is fed into Steganographic Decoder.

Types of Steganography

- **Text Steganography**
- **Image Steganography**
- **Audio Steganography**
- **Video Steganography**
- **Protocol Steganography**

Text Steganography
Text Steganography is hiding information inside the text files. It involves things like changing the format of existing text, changing words within a text, generating random character sequences or using context-free grammars to generate readable texts.

Image Steganography
Hiding the data by taking the cover object as the image is known as image steganography. In digital steganography, images are widely used cover source because there are a huge number of bits present in the digital representation of an image. There are a lot of ways to hide information inside an image.

Audio Steganography
In audio steganography, the secret message is embedded into an audio signal which alters the binary sequence of the corresponding audio file. Hiding secret messages in digital sound is a much more difficult process when compared to others, such as Image Steganography.

Video Steganography
In Video Steganography you can hide kind of data into digital video format. The advantage of this type is a large amount of data can be hidden inside and the fact that it is a moving stream of images and sounds.

Protocol Steganography
It is the technique of embedding information within network control protocols used in data transmission such TCP, UDP, ICMP etc. You can use steganography in some covert channels that you can find in the OSI model. For Example, you can hide information in the header of a TCP/IP packet in some fields that are either optional.

IV. DIGITAL WATERMARKING

Digital Watermarking is the use of a type of tag embedded in digital media such as audio, video or image that identifies the source or owner of the copyright. This process is used to track copyright infringement on social media and to determine the integrity of notes in the banking system. Digital watermark is some additional information embedded in a digital object for verification or integrity purposes. This could be, for example, text, logo, hash code, or other information. In many cases digital watermarking methods are used to protect the cover image itself, not the embedded information, because the embedded information

International Journal of Engineering& Scientific Research
Vol.10 Issue 02, February 2022
ISSN: 2347-6532 Impact Factor: 6.660
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

is not a secret message, but serves to identify the owner of the image or to control image integrity.

The removal of such information occurs when it is necessary to verify the identity of the image, to verify its authenticity, to check the existence of any random or deliberate distortions, while the main goal of steganographic embedding is to convey a hidden message to the recipient.

Digital watermarks are widely used in the field of copyright protection for digital content, in particular, digital photography: drawings, photographs. But digital watermarking techniques can also be used elsewhere, for example, to embed patient data on medical images. Many embedded algorithms not only allow you to detect changes in the image, but also to replicate them and restore the damaged area.

Types of Watermark

Visible Watermarks: These watermarks are visible.

Invisible Watermarks: These watermarks are embedded in the media and use steganography technique. They are not visible by naked eyes.

Public Watermarks: These can be understood and modified by anyone using certain algorithms. These are not secure.

Fragile Watermarks: These watermarks are destroyed by data manipulation. There must be a system which can detect all changes in the data if fragile watermarks are to be used.

V. EMBEDDING TECHNIQUES

Reversible Embedding

Implementing the embedding of information into digital images with a reversible embedding embediment. The real guideline for data encryption over the past few years is reversible embedding. Reversion means that after removing the embedded information, the original cover material can be restored to its original state. This feature is especially important for those applications where some sort of intelligent image processing containing embedded data is appropriate: fragmentation, pattern recognition, edge detection, etc. In this case, even with high visibility embedding, additional information contained in the image may distort the processing effect. Therefore, the only solution is to remove the embedded data and restore the cover image to its original state. Reverse embedded algorithms can work on both local data and frequency coefficients.

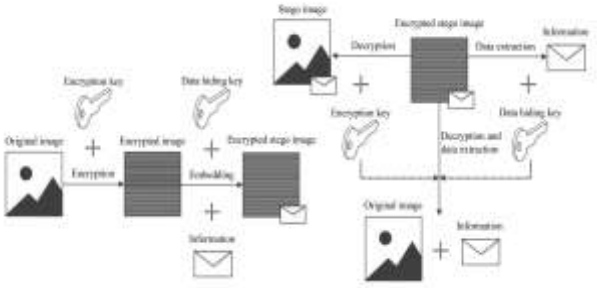

Figure 2 Reversible Information Embedding

Edge Detection Based Embedding

The additional information embedding in digital images using methods of steganography and digital watermarking in many studies is accompanied by the use of various approaches and techniques to increase the efficiency of embedding. A large number of studies in this area are based on the assertion that information embedding in some fragments of images is often more effective than in others.

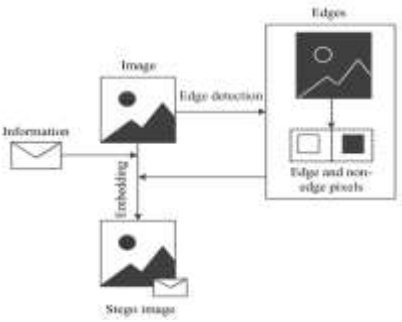

Figure 3 Edge Detection based Information Embedding

A common approach to increasing the imperceptibility of embedding is to hide data in the edges found in the image. To implement this approach, it is necessary to perform image pre-processing, which consists of edge detection in the image, as a result of which the image pixels will be defined as edge or non-edge.

CONCLUSION

The Existing methods of steganography and digital watermarking are actively evolving, and many researchers from different countries offer many new algorithms with different quality features. Despite the variety of advanced algorithms, in the field of digital embedding information, there are still many unresolved issues. The vast majority of modern embedded algorithms provide high embedding visibility, therefore, the attention of researchers working in this field should be aimed at achieving other indicators of functional embedding: retrieval, durability. Reviews have shown that work in these areas is ongoing, but there are still many problems that need new solutions.

REFERENCES

[1] H. Mostafa, A. F. Ali, and G. El Taweal, ``Hybrid curvelet transform and least signi_cant bit for image steganography," in Proc. IEEE 7th

Int. Conf. Intell. Comput. Inf. Syst. (ICICIS), Dec. 2015, pp. 300_305.

[2] M. Hamidi, M. E. Haziti, H. Cheri_, and M. E. Hassouni, ``Hybrid blind robust image watermarking technique based on DFT-DCT and Arnold transform," Multimedia Tools Appl., vol. 77, no. 20, pp. 27181_27214.

[3] A. K. Sahu and G. Swain, ``Reversible image steganography using dual-layer LSB matching," Sens. Imag., vol. 21, no. 1, p. 1, Dec. 2019.

[4] D. Hou, H.Wang,W. Zhang, and N. Yu, ``Reversible data hiding in JPEG image based on DCT frequency and block selection," Signal Process., vol. 148, pp. 41_47, Jul. 2018.

[5] P. Puteaux andW. Puech, "An ef_cient MSB prediction-based method for high-capacity reversible data hiding in encrypted images," IEEE Trans.Inf. Forensics Security, vol. 13, no. 7, pp. 1670_1681, Jul. 2018.

[6] G. Ma and J. Wang, ``Efficient reversible data hiding in encrypted images based on multi-stage integer wavelet transform," Signal Process., Image Commun., vol. 75, pp. 55_63, Jul. 2019.