DIGITAL WATERMARKING TECHNOLOGY IN INFORMATION SECURITY

[1]G. Naga Lakshmi, [2]P. Ruchitha, [3]G. Lavanya, [4]CH. Sai Greeshmanth, [5]R. Bhanu Prakash

[1] Assistant professor, Dept of ECE, DVR & Dr. Hs MIC college of technology, Andhra Pradesh, India
[2,3,4,5] Dept of ECE, DVR & Dr. Hs MIC college of technology, Andhra Pradesh, India

---

Abstract - *Watermarking technology has attracted more and more attention in various research fields Like information security. At this time, we protect the remote sensing data by using watermarking technology. As remote sensing data is delicate, it is necessary to enforce some management for authenticity and ownership. Particularly for the copyright protection, illegal use, and legitimacy identification of remote sensing image data. Therefore, this project proposes to use image watermarking technology to achieve comprehensive security protection of remote sensing image data, although the use of cryptography technology rises the applicability and security of watermarking technology. The remote sensing data is a representation of parts of the earth's surface as seen from space. The watermarking process is used for hiding digital information. A watermarking is a logo, text, or pattern. That is purposely covered in another image. Its purpose is to make it tougher for the original image to be imitative or used without authorization. Cryptography is the process of protecting information by transforming it into a secure format. Which provides an alternative solution for ensuring tamper resistance, and the ownership of intellectual property. And the tamper recognition will aware you when your device is being restricted by employees or other individual seeks. The untried results show that the arrangement of remote sensing image digital watermarking technology has good performance in the faintness and robustness of watermarking.*

***Key Words**: MATLAB, Satellite Image Detection, Digital Watermarking*

1. INTRODUCTION

In new years, every person's attention has traveled to the internet. It's a simple and fast way to send and access data and information all around the world. This information is mostly digital (text, images, audio, video). Everyone utilizes the internet, whether for personal or professional reasons. As a result, protecting user data from unauthorized access is vital. When did we get up back then? How can we prove that we own the information? To derive an explanation. A digital watermarking procedure is used to protect data so that it cannot be accessed or duplicated by an unauthorized person for malevolent purposes. A watermark is a piece of data included in digital media. The subject is a data-related portion of information. The proposed study looks at new ways for digital watermarking in both the spatial and transforms domains. The improvement in information technology has made it very simple to serve digital data. As time goes by, data sanctuary cobwebs get more protected. It is vital to protect multimedia data from attacks such as counterfeiting, piracy, and malicious alternation. Digital security can respond to a wide range of assaults and procedures. Watermarking is upper of them. A watermark is a label, tag, or information that seems on a document.

A watermark data is placed into digital media. The thing is a piece of data-related information (any label, citations, author name, id). The recommended investigation studies novel enhancements to digital watermarking methods in both the spatial and transform domains. The advancement of information technology has made the sharing of digital data quite simple. Data protection staleness becomes more secure as development progress. Protecting multimedia data from assaults such as counterfeiting, privacy, and malicious manipulation is critical. To provide a response to a large range of attacks and mechanisms. A watermark is an indication, a tag, or an information ampule that is injected into multimedia data to protect the original material from unauthorized change and distribution.

A digital watermark must be honestly unaffected by changes to the carrier signal in order to spot media files with copyright information. If accuracy is required, a fragile watermark would be used in its place. Steganographic techniques are used in steganography and digital watermarking to subtly encode data in earsplitting signals. Steganography and digital watermarking both use steganographic techniques to secrete data in noisy signals. Unlike steganography, which seeks faintness to human senses, digital watermarking prioritizes robustness. Digital watermarking is a submissive protection approach since a digital replica of data is identical to the original. It simply labels data without degrading it or restricting access to it.

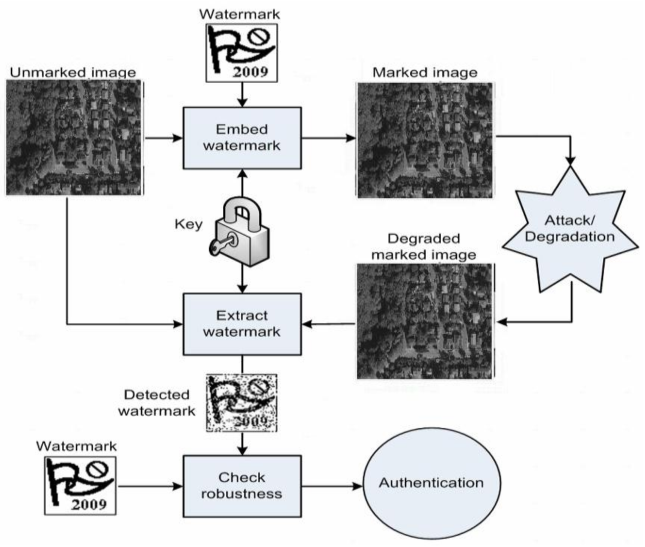
Source tracking is one application of digital watermarking. At each point of distribution, a watermark is placed in a digital signal. If a copy of the work is later discovered, the watermark can be extracted from the copy, and the distribution source can be determined. This method is said to have been used to track down the source that can be determined. This method is said to have been used to track down the source of illegally copied movies. Sources monitoring at each point of distribution, a watermark can be extracted from the copy-, and the determined. This method is said to have used been to track down the source of illegally copied movies.

2. FLOW CHART

2.1 Flow Chart

The inserting process inserts the watermark in the text reasonably and generates a watermark important. The flowchart of the proposed watermark embedding process is shown. The Image gaining process acquires the watermark image which can be the emblem, sign, or fingerprint of the original copyright owner….

Fig-1: Flow chart



2.EXPLANATION

2.2.1 HISTORY

The tenure "Digital Watermark" was created by Andrew Terkel and Charles Osborne in December 1992. The first successful embedding and extraction of a steganographic spread spectrum watermark were demonstrated in 1993 by Andrew Terkel, Charles Osborne.

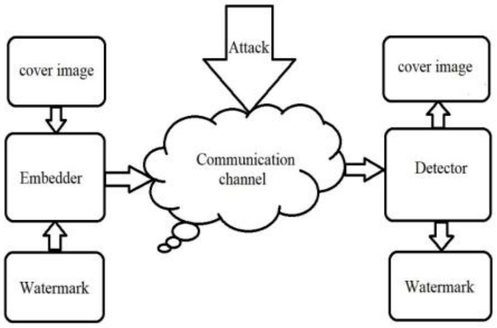
Watermarks are identification marks produced during the papermaking process. The first watermarks appeared in Italy during the 13th century, but their use rapidly spread across Europe. They stayed used as a resource to recognize the papermaker or the craft league that industrial the paper. The symbols often were created by a wire seamed onto the paper Mildew. Watermarks linger to be used today as producer's symbols and to avoid forgery.

2.2.2 General model for digital image watermark

A watermark embedder and a watermark detector are the two main components of the digital watermarking system. A watermark is put into the cover signal using a watermark embedder, and the existence of the watermark signal is detected using a watermark detector. During the development of embedding and noticing watermarks, a piece called a watermark significant is used. With the advancement of satellite remote sensing technology in recent years, remote sensing images have increasingly reflected their features of fast and easy access. Floating pictures and satellite pictures are the most common types of remote sensing images, which generally record geographic, environmental, resource, military, and other information vital to the national economy and people's confrontation. In rapports of land administration, figures show that by engaging satellite images, the time necessary for land merging is cut in half associated with outdated methods, and the cost is tens of times lesser.

As per the outcome, remote detecting images will play an important role in merging. Currently, remote sensing images are only employed as a spatial data input system for processing. The analysis and processing data are just saved as photos to complete the basic electrification. The initial remote sensing image and the processed image are both poorly protected. It is vital to pay attention not only to the safety of remote sensing pictures but also to their organization. Remote sensing image data is sensitive, so it is necessary to enforce some management for authenticity and ownership. In the sought-after, when companies have to obtain some data, watermarking can be used to foil illegal users from illegally dispensing and using data.

At the same time, watermarking technology can identify manipulation by remotely sensing data. The axiom "Digital watermarking" was designed by the inquiry labs, that invented this advanced technology. However, as photographers have been utilizing "watermarking" for a long time, this wording causes a lot of confusion in the digital photography world. These two types of "watermarking" are not substitutable.



3. DIGITAL WATERMARK LIFE CYCLE

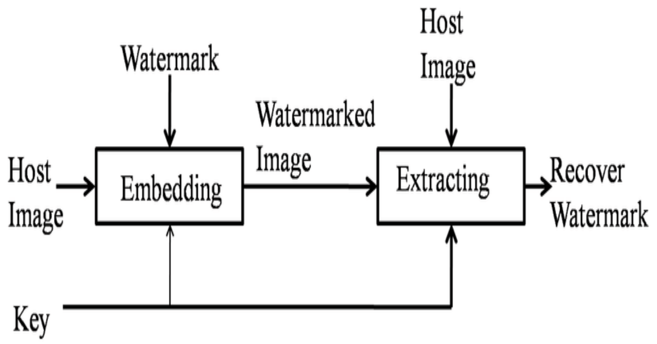
A digital watermark is a piece of information that will be embedded in a signal, while in some properties, the tenancy digital watermark mentions the difference between the watermarked signal and the cover signal. The host signal is the signal where the watermark will be inserted. Watermarking systems are usually broken down into three stages: embedding, attack, and detection. When an algorithm accepts the host and data to be embedded, it creates a watermarked signal.

At that point the watermarked fundamental signal is transmitted or kept, usually spread to another person. If this separate modifies, this is called an occurrence. Although the modification may not be mean, the tenure enchantment gets up from copyright protection applications, where tertiary revels may try to eliminate the digital watermark complete modification. There are numerous imaginable modifications, for example, a lossy firmness of the data (in which resolution is diminished), cropping an image or video, or intentionally adding noise.

Detection (also known as extraction) is a method that attempts to extract the watermark from the assaulted signal. The watermark is still present and can be recovered provided the signal was not altered during transmission. Uniform unknown the modifications remained simple, the withdrawal technique is robust digital watermarking systems should be able to produce the watermark appropriately. Any alteration to the signal should cause the extraction method to fail in fragile digital watermarking.

3.1 EMBEDDING

The way of watermark creation is using a watermarking critical and the watermarking algorithm, to yield the watermarked digital image. The inserting process vary based on which image domain is being processed, e.g., the terrestrial, incidence field, or the wavelets. Depending on the embedding method measurable (single-bit) or readable (multi-bit) watermarks are being incorporated into the digital images. A watermark implanting technique is a procedure for inserting a watermark into a coverup document.



3.2 WATERMARK ATTACKS

In watermarking vocabulary, an “attack” is any processing that may impair the detection of the watermark or communication of the information conveyed by the watermark. There are various types of attacks on watermarking schemes: Basic attacks, Removal Attacks, legal attacks, Geometric attacks, Protocol Attacks, and Cryptographic Attacks.

3.3 BASIC ATTACKS

Basic spells take advantage of strategy flaws in inserting techniques. Simple meal spectrum techniques, for example, can withstand amplitude and noise addition but are susceptible to timing errors. Because the technique relies on on-chip signal synchronization, adjusting the synchronization can result in the loss of embedded data. It is possible to change the length of an audio file without changing the pitch, which can be an effective attack on audio files.

3.4 LEGAL ATTACKS

Legal attacks refer to an attacker's ability to cast doubt on the watermarking scheme in court. These spells trust on present and future legislature on copyright laws and digital information ownership, the credibility of the owner and the attacker, the owner's financial strength versus the attacker's, expert witnesses, and the lawyers' capability. A truly robust watermarking scheme must limit an attacker's ability to call into question technical evidence presented in court.

3.5 REMOVAL ATTACKS

Removal sessions purpose at the complete elimination of the watermark data from the watermarked data without instant the security of the watermarking algorithm (e.g., without the crucial used for watermark embedding). That is, no allowance, even exorbitantly multifaceted, can recuperate the watermark information from the attacked data. This grouping contains denoising, quantization (e.g., for firmness), demodulation, and collusion fits. Not all of these approaches always come close to their goal of complete watermark removal, but they may damage the watermark information meaningfully.

3.6 COPYRIGHT ATTACK

Cryptographic attacks aim to break the security methods used in watermarking schemes, allowing the embedded watermark information to be removed or misleading watermarks to be embedded.

3.7 PROTOCOL ATTACKS

The effort to challenge the complete watermarking application thought. Invertible watermarks are used in one type of protocol attack. Inversion works by the attacker removing his watermark from the watermarked data and claiming ownership of the watermarked data. This can lead to confusion about who actually owns the data. The auxiliary eruption is another type of propriety attack. In this case, the goal is not to destroy or impair the detection of the watermark, but to approximate, a watermark from watermarked data and copy it to some extra data referred to as board verifications. The duplicate occurrence is used when a lawful watermark in the board data can be bent without algorithmic information of the watermarking technology or data of the goal statistics.

Etiquette attacks the determination of the aggressive comprehensive notion of the watermarking request. One type of decorum attack is based on the thought of invertible watermarks. The numeral overdue the transposal is that the aggressor withdraws his personal watermark since the watermarked data and autonomies to be the proprietor of the watermarked information. The copy occurrence is valid when a valid watermark in the goal data can be produced with neither algorithmic knowledge of the watermarking technology nor the knowledge of the watermarking key.

3.8 DETECTION

The watermark detection and extraction module determine whether or not the data contains a specified watermark and whether or not the watermark can be extracted. The module's input can be a banned image, a key, a watermark, or an original image, and the output can be a watermark or some kind of credibility value. It indicates the possibility of the data containing the specified watermark.

4. WAVELET TRANSFORM

The knowledge of wavelet transform and the collection of inserting incidence bands make use of the Hammer keep rottenness process. The image is fragmented into mouth features LHn, HLn, HHn and estimate constants LLC on N scales, and N=1, 2,...N. LL are the minutiae gotten after sieving in the bottommost frequency band. HH retains the detailed information after filtering in both level and vertical directions.

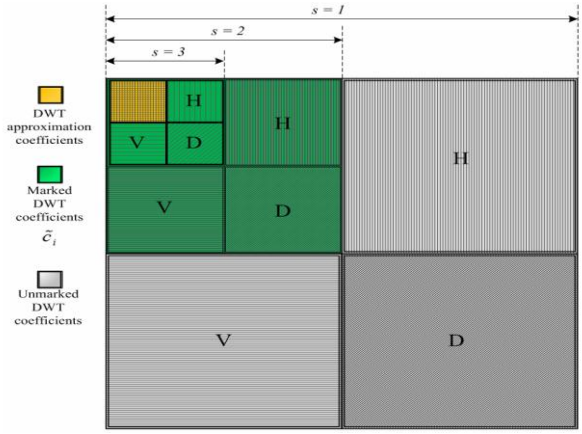


Fig: dwt coefficients for one 8x8 block image

5. SOFTWARE REQUIREMENTS MATLAB

MATLAB is a complex practical computation linguistic and collaborating environment for algorithm expansion, data imagining, data study, and mathematical computation. By means of MATLAB, you can crack technical calculation difficulties earlier than with old-style programming languages, such as C, C++, and Fortran.

MATLAB is a data analysis and visualization tool with extensive support for matrices and matrix operations. In total, MATLAB is an important programming language with unresolved design skills. One of the reasons MATLAB has become such an important tool is the use of collections of MATLAB programs designed to support a specific task. These collections of programs are mentioned as tool cabinets, and the image indulgence toolbox is of particular interest to us. To some extent than interpreting all of MATLAB's skills, we will frontier ourselves to that business with image management. As wanted, we will familiarize functions, instructions, and methods. A MATLAB function is a keyword that accepts various parameters and returns some type of output, such as a matrix, string, or graph. Such purposes contain sin, im-read, and im-close. There are many functions in MATLAB, and as we will see, writing our own is simple (sometimes necessary). The atmosphere is the typical statistics type in MATLAB, and all data are assumed to be matrices of some kind. Images, of course, are matrices with grey values (or possibly RGB values) as their elements. MATLAB considers single values to be matrices, whereas a string is simply a matrix of characters, the length of which is the string. We will aspect at the more general MATLAB commands in this chapter, and we will discuss images in later chapters. When you start up MATLAB, you have a blank window called the Command Window_ in which you enter commands. Given the huge quantity of MATLAB connotations and the varied strictures they can revenue, a command-line style boundary is much more efficient than a complex sequence of pull-down menus.

You can use MATLAB in a wide range of applications, including signal and image processing, communications, control design, test and measurement financial modeling, and analysis. Add-on tool chest (collections of special-purpose MATLAB functions) spread the MATLAB situation to solve precise lessons of hitches in these application areas. MATLAB provides many landscapes for documenting and allocating your work. You can integrate your MATLAB code with other languages and claims, and distribute your MATLAB procedures and applications.

Once occupied with imageries in MATLAB, there are many clothes to retain trendy attention such as lading an image, using the precise process, transferrable the data as dissimilar data types, how to show an image-, and changing between different image setups. Image Dispensation Tool chest transports a comprehensive set of reference-standard procedures and graphic tools for image allowance, analysis, picturing, and procedure development. You can achieve image improvement, image deblurring, feature detection, noise reduction, image division, spatial alterations, and image registration. Many determinations in the tool breakfront are multithreaded to take the benefit of multicore and multiprocessor computers. and graphic tools for image processing, examination, visualization, and algorithm development. Your canister complete dual increase, image deblurring, feature detection, sound decrease, image subdivision, spatial transformations, and image registration. Many meanings in the tool chest are multithreaded to take gain of multicore and multiprocessor computers.

6. IMAGE TYPE CONVERSION

·RGB Image to Intensity Image (rgb2gray)

·RGB Image to Indexed Image (rgb2ind)

·RGB Image to Binary Image (im2bw)

·Indexed Image to RGB Image (ind2rgb)

·Indexed Image to Intensity Image (ind2gray) ·Indexed Image to Binary Image (im2bw)

·Intensity Image to Indexed Image (gray2ind) ·Intensity Image to Binary Image (im2bw)

·Intensity Image to RGB Image (gray2ind, ind2rgb)

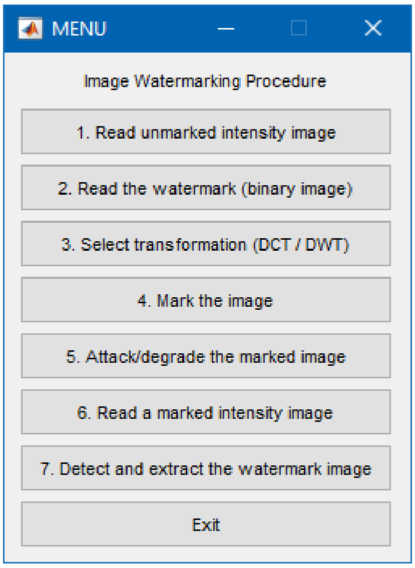
7. PROCEDURE AND INTERFACE IN MATLAB

1. Read unmarked intensity image,
2. Read the watermark (binary image),
3. Select transformation (DCT / DWT),

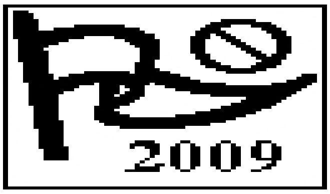
   Mark the image,

4. Attack/Degrade the marked image,
5. Read a marked intensity image,
6. Detect and extract the watermark image,
7. Exit

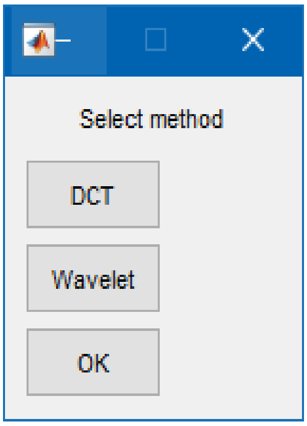
7.1 Read unmarked intensity image


MENU
Image Watermarking Procedure
1. Read unmarked intensity image
2. Read the watermark (binary image)
3. Select transformation (DCT / DWT)
4. Mark the image
5. Attack/degrade the marked image
6. Read a marked intensity image
7. Detect and extract the watermark image
Exit

7.2 Read the watermark

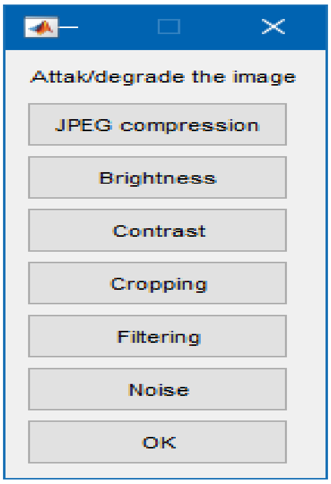


7.3 DCT/DWT Select transformation



7.4 Mark the image

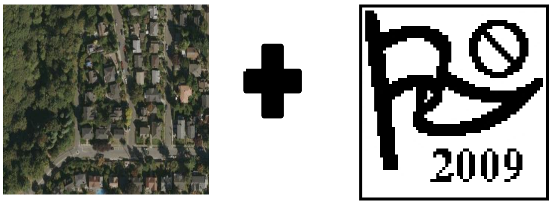
7.5 Attack/Degrade the marked image



7.6 Read a marked intensity image

If the information is implanted in the unique image, the strength of the communicated image is designed. If there is binary data fixed in the image, the development continues otherwise, the image contains no data.

7.7 Detect and Extract the watermark image



7.8 Appendix

Appendix B includes references, as well as research papers from which we derived the foundational research for this project.

8. ACKNOWLEDGEMENTS

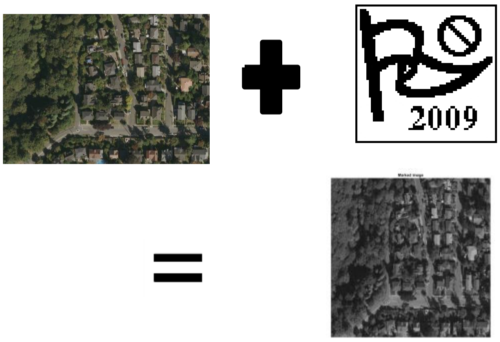
I'd like to take this time to thank the individuals listed below for their invaluable charities and support with this project. Originally, I would like to recognize my project manager, Ms. **G. Naga Lakshmi, M. Tech** for his guidance and support, especially for the valuable ideas and knowledge provided throughout the Project. Her skill and knowledge in **communication and signal process** make valuable comments and suggestions that have been very useful in solving problems encountered during the Development.

I stay thankful to **DR. K. SRINIVAS**, Principal, and Prof. **D. PANDURANGA RAO**, CEO, for providing me with the opportunity to complete this project. I also extend my thanks to all faculty members of **Electronics and Communication Engineering** faculty members for their valuable guidance and encouragement in this Development.

I would identical to pick my honest thanks to all my groups for unraveling their data, valuable contributions, and help with this Development.

Finally, I want to express my gratitude to my family for their unwavering support and assistance during my academic career and for their ongoing support and encouragement of this progress.

8. RESULT



10.CONCLUSION

At present-day data can be replicated simply due to the collaboration and alphanumeric communication of software data. This material makes alphamerical image watermarking a significant field of inquiry.

Digital image watermarking using many methods has been valuable as a significant tool for image authorization, honesty verification, restricted detection, copyright safety, and digital safety of an image.

Furthermore, to improve strength along with security, researchers should focus on evolving new, advanced techniques.

11. REFERENCE

[1] Z.L. Zhou, C.N. Yang, B.J. Chen, X.M. Sunbathe, Q. Liu, Q.M.J. Wu, Effective and efficient image reproduction finding through hostility to subjective spin, IEICE Trans. Inf. Syst. E99-D (6) (2016) 1531-1540.

[2] C. Qin, C.C. Chang, P.Y. Chen, Self-embedding fragile watermarking with healing functionality primarily based totally on adaptive bit allocation mechanism, Signal Process. 92 (4) (2012) 1137–1150.

[3] J. Li, X.L. Li, B. Yang, X.M. Sun, Segmentation-primarily based picture copy-pass forgery detection scheme, IEEE Trans. Inf. Forensics Secure. 10(3) (2015)507-518.

[4] J.W. Wang, T. Li, Y.Q. Shi, S.G. Lain, J.Y. Ye, Forensics characteristic evaluation in quaternion wavelet area for distinguishing photographic snapshots and pc graphics, Multimedia Tool Appl. (2016).

http://dx.doi.org/10.1007/s11042-016-4153-0.

[5] C. Qin, X.Q. Chen, D.P. Ye, J.W. Wang, X.M. Sun, A novel picture hashing scheme with perceptual robustness the usage of block truncation coding, Inform. Sci. 361–362 (2016) 84–99.

[6] C. Qin, P. Ji, X.P. Zhang, J. Dong, J.W. Wang, Fragile picture watermarking with pixel-smart restoration primarily based totally on overlapping embedding strategy, Signal Process. 138 (2017) 280–293. [7] Y.Q. Shi, X.L. Li, X.P. Zhang, H.T. Wu, B. Ma, Reversible facts hiding: Advances withinside the beyond decades, IEEE Access 4 (2016) 3210–3237.

[7] C. Qin, C.C. Chang, T.J. Hsu, Reversible facts hiding scheme primarily based totally on exploiting modification path with steganographic snapshots, Multimedia Tools Appl. 74 (15) (2015) 5861– 5872.

[8] L.X. Luo, Z.Y. Chen, M. Chen, X. Zeng, Z. Xiong, Reversible picture watermarking the usage of interpolation technique, IEEE Trans. Inf. Forensics Secure. 5 (1) (2010) 187– 193. [10] C. Qin, Y.C. Hu, Reversible facts were hiding in VQ index desk with lossless coding and adaptive switching mechanism, Signal Process. 129 (2016) 48–55.

[9] LX, Luo, Z.Y. Chen, M. Chen, X. Zeng, Z. Xiang. Revocable image watermarking using exclamation technique, IEEE Trans. Inf. Forensics Secure. 5 (1) (2010) 187– 193. [10] C. Qin, Y.C. Hu, Revocable information beating in VQ directory table with lossless coding and adaptive switch device, Indication Procedure. 129(2016) 48–55.