Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol 3, No.7, 2012


# A Study of Image Fingerprinting by Using Visual Cryptography

Santosh Choudhary, Shrikrishan Yadav*, Neeta Sen, Gosiya Nasreen
Pacific College of Engineering, Pacific University, Udaipur-313001, Rajasthan, India
* E-mail of the corresponding author

**Abstract**

As digital media has made our life more colourful because of its advantages like easier to access, copy and distribute. But as what we have seen, series of malice activities like copyright infringement, counterfeiting, piracy and information distortion make damages to both the producers and the users of digital products. So we really need some technology to protect the copyright, authenticity, integrity of the digital products and the intellectual property of the users. There are many techniques such as Digital watermarking and Visual Cryptography both have been widely used for protection of data either in text, video, sound or digital images form in modern network time. Digital watermarking is an evolving field that requires continuous effort to find for the best possible method in protecting multimedia content. But Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. Both techniques addresses the growing concerns of theft and tampering of digital media through the use of advanced signal processing strategies to embed copyright and authentication information within media content in their respective manner. In this paper we have discussed image fingerprinting with the help of visual cryptography technique.

**Keywords:** Authentication, Digital Media, Digital Watermarking, Fingerprinting, Image, Piracy, Visual Cryptography

## 1. Introduction

With the growth of the Internet, more and more information is being transmitted in digital format (image, audio, video, etc.) now than ever before. However, the greatest drawback in transmission of digital information is its easy weakness to have innumerable copies of the same nature and quality as that of the original. So, there is always the chance of lack of authentication, ownership proof and copyright protection. Therefore, various cryptography algorithms and embedding techniques have been established to solve this type's problems that stress on copyright marking. Some message is secretly inserted within the original digital message and that secret message is used to emphasize copyright over the host digital message. But all such algorithms must satisfy a number of requirements to maintain the quality and integrity of the resultant information. The watermarking and visual cryptography both techniques are used to secure or protect or hide data from unauthorized users.

## 2. Digital Watermarking

Watermarking is the process of embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners, in the same manner as paper bearing a watermark for visible identification. In digital watermarking, the signal may be audio, pictures, or video, in which a pattern of bits inserted into a digital image, audio or video file that identifies the file's copyright information (author, rights, etc.) If the signal is copied, then the information also is carried in the copy. A signal may carry several different watermarks at the same time. Digital watermarking is also called data embedding and information hiding. Digital

 

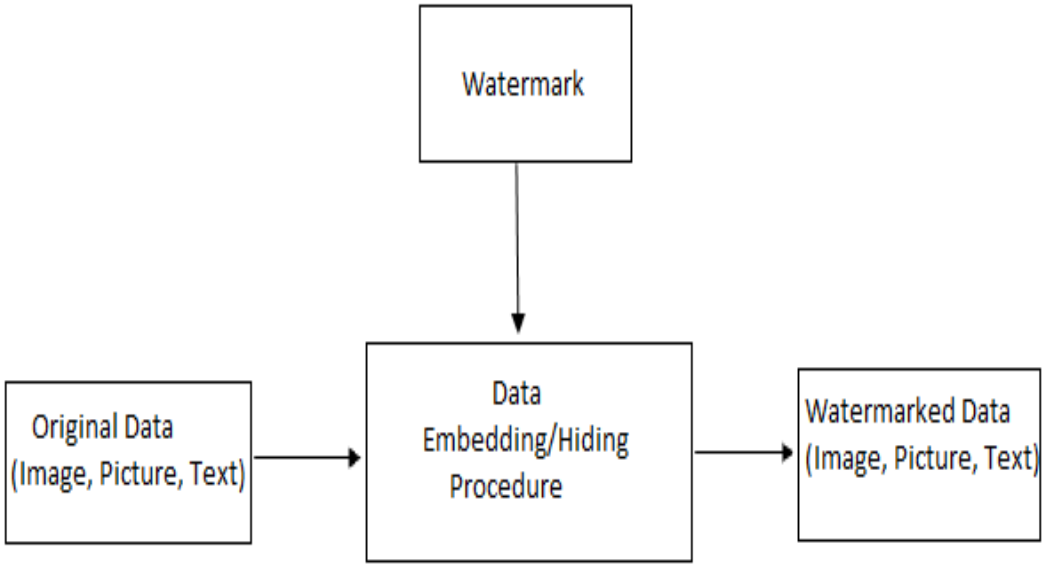


Figure 1. Block Diagram of Watermarking Technique

Watermarking technology is an emerging field in computer science, cryptography, signal processing and communications. According to Human Perception there are two types of watermarking, visible and invisible.

In visible digital watermarking, the information is visible in the picture or video. Typically, the information is a text or a logo, which identifies the owner of the media. The image on the right has a visible watermark. For example when a television broadcaster adds its logo to the corner of transmitted video, this also is a visible watermark. The logo of the broadcaster such as Zee, Sony, ESPN and National Geographic etc is mainly on the right top corner of the television, which is visible to every user.

In invisible digital watermarking, information is added as digital data to audio, picture, or video, but it cannot be professed as such. The watermark may be projected for widespread use and thus, is made easy to retrieve or, it may be a form of steganography, where a party communicates a secret message embedded in the digital signal. In either case, as in visible watermarking, the objective is to attach ownership or other descriptive information to the signal in a way that is difficult to remove. It also is possible to use hidden embedded information as a means of covert communication between individuals.

One application of watermarking is in copyright protection systems, which are intended to prevent or frighten unauthorized copying of digital media. In this use, a copy device retrieves the watermark from the signal before making a copy; the device makes a decision whether to copy or not, depending on the contents of the watermark. Another application is in source tracing. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies. Annotation of digital photographs with descriptive information is another application of invisible watermarking. While some file formats for digital media may contain additional information called metadata, digital watermarking is distinctive in that the data is carried right in the signal.

 

2.1Elements of a Watermarking System

A watermarking system can be viewed as a communication system consisting of three main components: an embedder, a communication channel and a detector. Watermark information is embedded into the signal itself, instead of being placed in the header of a file or using encryption like in other security techniques, in such a way that it is extractable by the detector. To be more specific, the watermark information is embedded within the host signal before the watermarked signal is transmitted over the communication channel, so that the watermark can be detected at the receiving end, that is, at the detector. A general digital watermark life-cycle has different phases which are embedding, attacking, detection and retrieval functions. The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the host signal. A watermarking system shown in fig. 2 is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal.

Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. While the modification may not be malicious, the term attack arises from copyright protection application, where pirates attempt to remove the digital watermark through modification. There are many possible modifications, for example, Lossy compression of the data, cropping an image or video or intentionally adding noise. Detection often called extraction is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted. In robust digital watermarking applications, the extraction algorithm should be able to produce the watermark correctly, even if the modifications were strong. In fragile digital watermarking, the extraction algorithm should fail if any change is made to the signal. Thus the robust digital watermarking is better as compare to fragile because the watermark can be extract even if the information is modified strongly by unauthorized users.

Watermarking is always regarded as a subset of steganography. However, the message hidden in watermarking is not the major information that we want to convey. On the converse, the information hidden in steganography is always the most important. Because of invisibility, what is hidden in both watermarking and steganography is the existence of the signal. However, for the cryptography, what is hidden is the content of information.

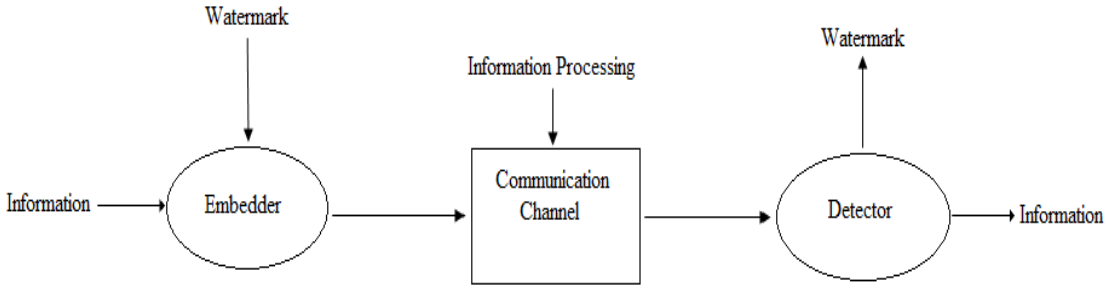


Figure 2. General Watermarking Systems

 

## 3. Visual Cryptography

Visual Cryptography is a secret sharing scheme that uses the human visual system to perform computations. It is a new type of cryptography technique in which no cryptographic computations is needed as the decryption end. The secret sharing was invented independently by Adi Shamir.

The cryptography was generalised to visual cryptography by Mony Naor and Adi Shamir in 1994. When the random image contains truly random pixels it can be seen as a one-time pad system and will offer unbreakable encryption. In the overlay animation you can observe the two layers sliding over each other until they are correctly aligned and the hidden information appears. To try this, you can copy the example layers 1 and 2 given in fig. 3, and print them onto a transparent sheet or thin paper.

Always use a program that displays the black and white pixels correctly and set the printer so that all pixels are printed accurate. You can also copy and paste them on each other in a drawing program like paint and see the result immediately, but make sure to select transparent drawing and align both layers exactly over each other. Therefore, the protection of rightful ownership of digital data has become an important issue in recent years. Nowadays, many researchers are working and have proposed many techniques to protect the intellectual property rights for digital images or information. So both methods are used to hide a meaningful data, in a host image for the purpose of copyright protection, integrity checking, and captioning.

It is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. Visual Cryptography uses the basic technique to hide information in which it uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Both transparent images and layers are required to reveal the information.

### 3.1 Implementation of Visual Cryptography when Information is in Image Form

It is easy to implement visual cryptography to secure data when it is in image form. In the visual cryptography, if the information is in images form than it works like this. Each pixel of the images is divided into smaller blocks. There are always the same number white (transparent) and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks. The example images from above uses pixels that are divided into four parts.

In the fig. 3 we can see that a pixel, divided into four parts, can have six different states. If a pixel on layer 1 has a given state, the pixel on layer 2 may have one of two states: identical or inverted to the pixel of layer 1. If the pixel of layer 2 is identical to layer 1, the overlaid pixel will be half black and half white. Such overlaid pixel is called grey or empty. If the pixels of layer 1 and 2 are inverted or opposite, the overlaid version will be completely black. This is an information pixel.

We can now create the two layers. One transparent image, layer 1, has pixels which all have a random state, one of the six possible states. Layer 2 is identical to layer 1, except for the pixels that should be black (contain information) when overlaid. These pixels have a state that is opposite to the same pixel in layer 1. If both images are overlaid, the areas with identical states will look gray, and the areas with opposite states will be black. The system of pixel can be applied in different ways. In our example, each pixel is divided into four blocks. However, you can also use pixels, divided into two rectangle blocks, or even divided circles. Also, it doesn't matter if the pixel is divided horizontally or vertically. There are many different pixel systems, some with better contrast, higher resolution or even with colour pixels. The pixels size or colour and resolution can be used according the requirements of the condition or problem.

In fig.3 the outcomes 12 are given but the overlaid or combination of empty pixel and information pixel can be done in many ways. If the pixel states of layer 1 are truly (crypto secure) random, both empty and information pixels of layer 2 will also have completely random states. One cannot know if a pixel in layer 2 is used to create a grey or black pixel, since we need the state of that pixel in layer 1 (which is random) to know the overlay result. If all

 

requirements for true randomness are fulfilled, Visual Cryptography offers absolute secrecy according to the Information Theory.

If Visual Cryptography is used for secure communications, the sender will distribute one or more random layers 1 in advance to the receiver. If the sender has a message, he creates a layer 2 for a particular distributed layer 1 and sends it to the receiver. The receiver aligns the two layers and the secret information is revealed, this without the need for an encryption device, a computer or performing calculations by hand. The system is unbreakable, as long as both layers don't fall in the wrong hands. When one of both layers is intercepted it's impossible to retrieve the encrypted information.

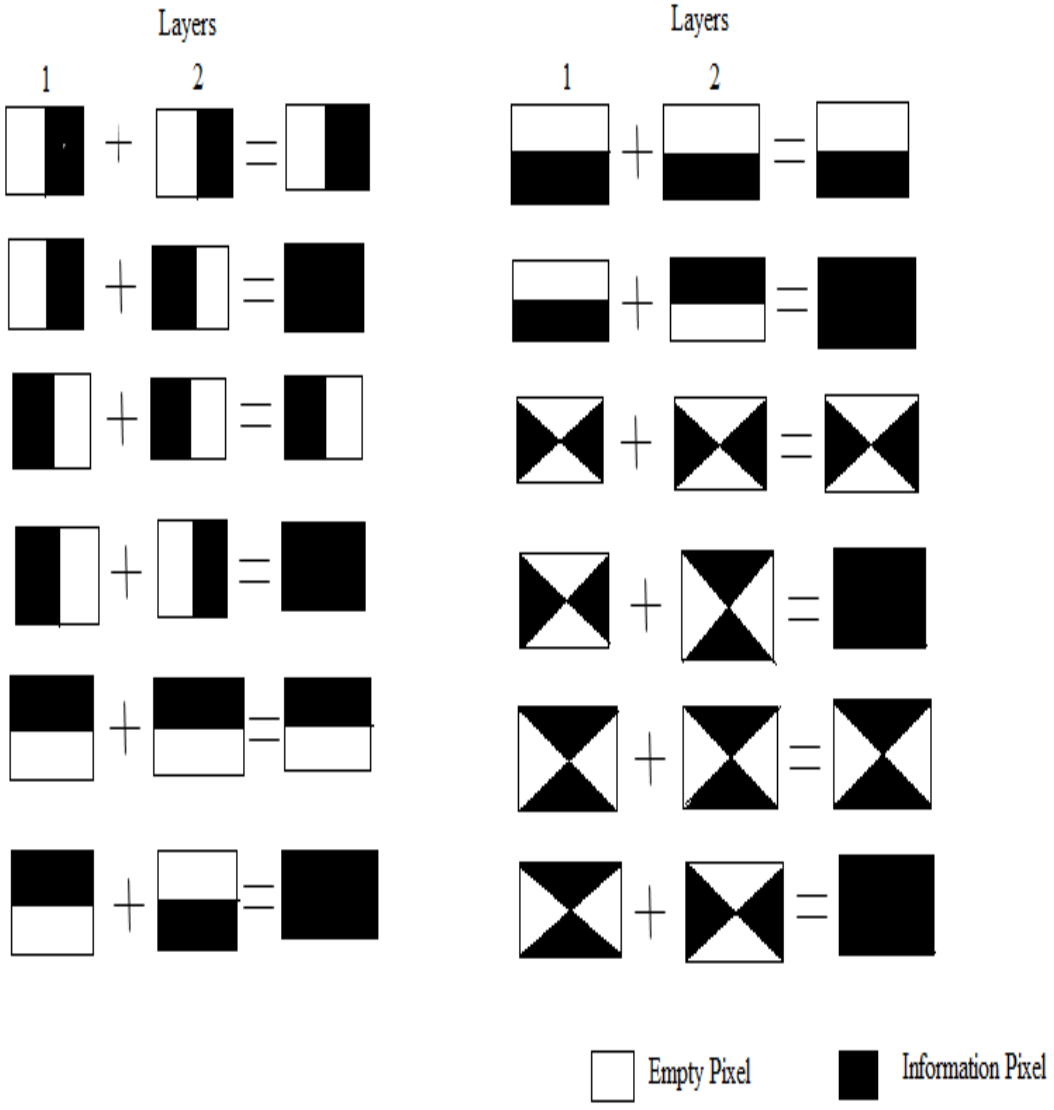


Figure 3. Two Image Layers Overlapping to Secure Data

3.2 Implementation of Visual Cryptography by using Fingerprinting

Fingerprinting of an image is a method by which the information related to the image and its owner can be kept

 

hidden in the image (cover image) itself. A unique image identification number, customer id and name of the image will be used as the fingerprint of each image buy-sell transaction. This unique fingerprint will be embedded into that particular image. The fingerprint will be generated using a text to image conversion algorithm by which secret data will be prepared. The novelty of the algorithm lies in the fingerprinting method. It is visually encrypted to enhance the security. The fingerprint is divided into some shares of equal size which alone does not contain any significant information about the fingerprint unless they are visually overlapped one above the other. The complete information in the fingerprint is divided equally among all the shares.

It is visually encrypted to enhance the security. The fingerprint is divided into some shares of equal size which alone does not contain any significant information about the fingerprint unless they are visually overlapped one above the other. The complete information in the fingerprint is divided equally among all the shares. To serve the fingerprinting purpose the shares are embedded into the image in different blocks in the frequency domain. A single cover image will contain all the shares of the fingerprint. So whole information about the fingerprint is inside the cover image but embedded into different spatial locations. This involves a new strategy of embedding multiple watermarks in the same image. Each share can be seen as an independent watermark and will be embedded into a different block of the image.

The method proposed here is supposed to be very robust. The fingerprint is secure against the general image processing attacks like noise addition and image compression. The main advantage of using a visually encrypted fingerprint is that there is no effect of the normal correlation of the fingerprint to the image. Blind detection of the fingerprint to illegally detect it is not possible since the correlated fingerprint will appear as noise only. Even some shares of the fingerprint get detected but without the successful detection of every share it is impossible to regenerate the fingerprint. So no illegal person can detect the fingerprint without knowing the all the shares altogether.

**Generation of fingerprint:** The logos of organizations or some standard images have been used by the watermarking fraternity worldwide. But these are not image and customer dependent, which is the basic need for a fingerprint. So what we propose here to generate a unique fingerprint for every image. This fingerprint will contain in information about the customer and the image itself in the form of text. This text will be converted into image which will finally be used as a fingerprint.

**Visual cryptography:** This is a very popular strategy to encrypt the images. The image is divided into some number of equally sized shares. Individual shares do not contain any information. They all appear as noise. The only way to extract the original image information is to overlap over each other. We are going to visually encrypt our fingerprint into 4 shares. These shares will be embedded into the image not the original fingerprint as it is done in all the watermarking strategies.

**Averaged Block based DCT Fingerprinting:** This technique is far advanced and beneficial than the classical mid band coefficients exchange scheme. Since the coefficients in which the watermarking information is entered are unique in every image, so it is very difficult for the users to collude the fingerprint and its embedding location in the image.

**Multi-fingerprint Algorithm:** The general watermarking techniques embed only one watermark into the image. Some have watermarked the image using more than one watermark but in a sequential manner, i.e. next watermark is embedded into the image in the coefficients returned by first watermarking steps. This is not effective way to do so, since if one watermarking algorithm fails then the whole chain of watermarks is lost. Also the noise added to the image is very high. But we propose the multi-fingerprint Algorithm in which different shares generated through visual cryptography will be embedded into the image at different spatial location altogether.

3.2.1 Proposed Steps to Secure Information in Cover Image in Visual Cryptography with Fingerprint

Step1: Generate Watermarked Image by Using Visual Cryptographic Encryption

1. Start

2. Take a Cover Image

 

3. Subdivision of Image into four parts LL, LR, UR, and UL (As shown in Fig. 3)
4. Apply DCT method using mid-band coefficient

Step 2: Generation of Fingerprint
1. Start
2. We take input data in form of text data for example consumer id, unique image no., image name etc
3. This secure information is embedded into cover image
4. Then we get watermarked secure image

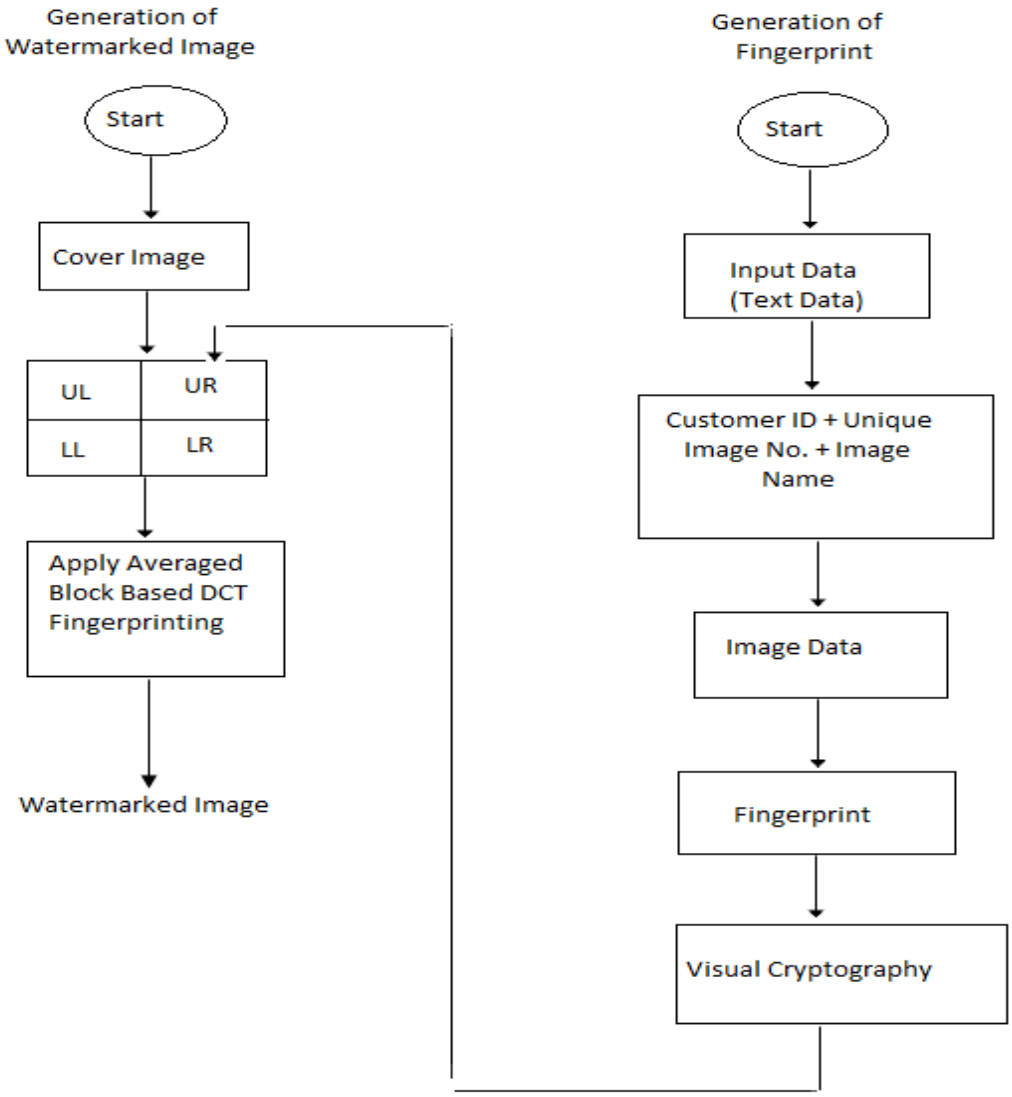


Figure 4. Proposed Flow Chart for Visual Cryptography with Fingerprint

 

## 4. Conclusion and Future Scope

The digital watermarking and visual cryptography methods are used to hide or protect information from unauthorized users to maintain the privacy and originality. The field of digital watermarking is young and there are some anticipated limitations, it has potential and some unique features which other alternatives lack. Also, it will be fruitful if the connection between data hiding and cryptography is further investigated in future.

The information hiding in visual cryptography can be applied to many applications in real and cyber world. The advantage is that the final decryption process is done by human visual system instead of complex computations, so it is less complex to implement as compare digital watermarking. The techniques will have a significant effect on defence, business, copyright protection and other fields where information needs to be protected at all costs from attackers. Intelligent Watermarking Techniques will be of great value to undergraduate and postgraduate students in many disciplines, including engineering and computer science. It is also targeted at researchers, scientists and engineers.

## References

S.P. Mohanty, et aI., "A Dual Watennarking Technique for Images", Proc. 7th ACM International Multimedia Conference, ACM-MM'99, Part 2, pp. 49-51, Orlando, USA, Oct. 1999.

Mahmoud El-Gayyar, Watermarking Techniques Spatial Domain Digital Rights Seminar, Germany, may 2006

Naor, M. and Shamir, A. 1995. Visual Cryptography. *Advances in Cryptography-Eurocrypt*, 950: 1-12.

Shamir, A. 1979. How to Share a Secret. *Communications of the ACM*. 22: 612-613.

J. Cox, M. L. Miller, and J. A. Bloom, Digital Watermarking. Morgan Kaufmann Publishers, 2002.

M. Kutter and F. Hartung, "Image watennarking techniques," to appear in Proceedings of the IEEE, Special Issue on Identification and Protection of Multimedia Infonnation, 1999.

J. Cox, "Spread-spectrum techniques for image watennarking," to appear in Proceedings of the IEEE, Special Issue on Identification and Protection of Multimedia Infonnation, 1999.

Yusnita Yusof and Othman O. Khalifa. "Digital Watennarking for Digital Images Using Wavelet Transfonnation" appear in proceeding of the IEEE pp.665-669, April -2007 Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.

Akio Miyazaki and Akihiro Okamoto, “Analysis of watermarking systems in the frequency domain and its applications to design a robust watermarking system”, IEEE Transaction, pages 1969-1972, 2001.

Tan Liang, Fang Zhi-jun, “An adaptive middle frequency embedded Digital watermarking algorithm based on DCT domain”, IEEE Transaction, pages 382- 385, 2008.

Sandeep Katta, Recursive Information Hiding in Visual Cryptography Department of Computer Science, Oklahoma State University Stillwater, OK 74078

Stinson, D. 1995. Cryptography Theory and Practice. *CRC Press*.

R. J. Hwang and C. C. Chang, "Hiding a picture in two pictures," *Optical Engineering*, vol. 40, no. 3, 2001, pp. 342-351.

M. Naor and A. Shamir, " Visual cryptography, " *Eurocrypt'94*, *Lecture Notes in Computer Science*, Springer- Verlag, 1994, pp.1-12.

N.Nikolaidis and I.Pitas, “Robust image watermarking in the spatial domain”, *Signal Processing* vo1.66, 1998, pp.385-403.

Da-Chun Wu and Wen-Hsiang Tasi, “Image Hiding in Spatial Domain Using An Image Differencing Approach”, *Proc. Of* 1998 *Workshop on Computer Vision, Graphics, and Image Processing,* Taipei, Taiwan, pp. 280-287, 1998.

R. Wolfgang and E.J. Delp, ”A Watermark for Digital Image,” *IEEE int. Conf On Image Processing,* Lausanne,

 

Switzerland, September 1996, vol. 111, pp2 19-222.

Chiou-Ting Hsu and Ja-Ling Wu, "Multiresolution Watermarking for Digital Images", *IEEE Trans. Circuits and System II,* August 1998, vol. 45, no. 8

P.Y. Lin, J.S. Lee and C.C Chang, "Dual Digital Watermarking for Internet Media Based on Hybrid Strategies", IEEE Transactions on Circuits and Systems for Video Technology, vol. 19, pp. 1169-1177, 09.

C.C. Chang, Y.Z. Wang, C.S. Chan, "An Efficient Probability-Based t out of n Secret Image Sharing Scheme", Second International Conference on Future Generation Communication and Networking Symposia, FGCNS '08, vol.3, pp.121-124, 2008.

V. Saxena, J.P Gupta, "Collusion Attack Resistant Watermarking Scheme for Colored Images using DCT", IAENG International Journal of Computer Science, 34:2, IJCS-34-2-02.

**Mrs Santosh Choudhary:** received her B.E. degree in Computer Science and Engineering from Modi Institute of Technology, India and M. Tech in Computer Science & Engineering. She is pursuing Ph.D degree in "Image processing" from Pacific University, Udaipur. She has currently associate professor & HOD in Pacific College of Engineering, Udaipur, India and having more than 5 year teaching experiences. She guided many M. Tech scholars and presented more than 5 papers in International and National conferences. Her current research interests include Image Processing, Fuzzy Logic, Wireless Sensor Network and Data Structure.

**Shrikrishan Yadav:** working as an Assistant Professor in Computer Science and Engineering Department in PAHER University, Udaipur, India. He has completed B. E. in Computer Science and Engineering from Mohanlal Shukhadia University, Udaipur and pursued M.Tech. in Information Communication from Gyan Vihar University, Jaipur. He has more than three years of teaching experience. He is also published and presented 16 papers in International and National journals and conferences. He is an associate member of Computer Society of India (CSI), a member of International Association of Engineers (IAENG), International Association of Engineers and Scientists (IAEST), International Association of Computer Science and Information Technology (IACSIT) and Universal Association of Computer and Electronics Engineers (UACEE). His current research interest includes Cognitive Radio, Wireless Sensor Networks, Artificial Intelligence, Information Communication, and Wireless Communication System.

**Neeta Sen:** received her B.Sc degree in Computer Science from Mohanlal Shukhadia University (MLSU), Udaipur India and master degree in computer application form MLSU, Udaipur. She is pursuing Ph.D degree in "Digital Watermarking" from Pacific University, Udaipur. She is currently working as Senior Lecturer in Pacific College of Engineering, Udaipur, India and having more than 3 year teaching experiences. She presented and published more than 3 papers in International and National conferences. Her current research interests include Digital Watermarking, Networking, Compiler, Computer Architecture, and Software Engineering.

**Gosiya Nasreen: :** received her B. Tech. degree in Computer Science and Engineering from Rajasthan Technical University (RTU), Kota, India and pursuing master degree in computer science and engineering form Pacific University, Udaipur. She is currently working as Lecturer in Pacific College of Engineering, Udaipur, India and having more than 1 year teaching experiences. She presented and published more than 3 papers in International conferences. Her current research interests include Web Services, Operating System, Embedded System, and Software Engineering.