International Journal of Advanced Computer and Mathematical Sciences
ISSN 2230-9624. Vol 3, Issue 1, 2012, pp 194-204
http://bipublication.com

OPTICAL WATERMARKING FOR PRINTED DOCUMENT AUTHENTICATION

***D. D. Kamble, M. R. Dixit**

**R and D Department, Integral Technologies Pvt Ltd, Pune, M.S., India;*
Phone: 9970225742; Email:dhanashri.kamble@gmail.com
Department of Electronics and Telecommunication Engg,
KIT's college of Engg, Kolhapur, M.S., India; Phone: 9423859739;Email:mrdixit@rediffmail.com

ABSTRACT

The article describes a novel visual information concealment technique, referred to as optical watermarking, for the authentication of original printed documents. An optical watermark is a two-dimensional binary image. The optical watermark is constructed by the superposition of multiple two-dimensional binary images (referred to as layers), each with different carrier structural patterns embedding various hidden information. The hidden information is embedded into each layer using phase modulation. Based on properties of the human visual system and modulation principle, the hidden information becomes visible to the human eyes only when a right "key" is positioned on top of the optical watermark with the right alignment. Here, "keys" play the similar role as keys in encryption, that is, to decode hidden information. Due to its high security and tight link with electronic document systems, which requires documents to be finally printed on paper, the optical watermark has been applied to various electronic document systems. These are online ticketing, online bill of lading, and remote signing and printing of documents, where critical and unique information are embedded in watermarks and printed together with individual documents for future authentication. It has also been used in offline and traditional antiforgery applications, such as brand protection, reprinted high-value tickets, and identification documents.

Keywords: *Integrity verification; secret share; Phase Modulation; Dot Array; Data Hiding; Demodulation.*

1. INTRODUCTION

Information hiding techniques have recently become important in a number of application areas. Digital audio, video and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copy right notice or serial number or even help to prevent unauthorized copying directly. Military communications systems make increasing use of traffic security techniques which, rather than merely concealing the content of a message using encryption, seek to conceal its sender, its receiver, or its very existence. Similar techniques

are also used in some mobile phone systems. Criminals try to use whatever traffic security properties are provided intentionally or otherwise in the available communications systems, and police forces try to restrict their use. However, many of the techniques proposed in this young and rapidly evolving field can trace their history back to antiquity, and many of them are surprisingly easy to circumvent. Present work gives an overview of the field and it may be applied to various electronic document systems. These are online ticketing, online bill of lading, and remote signing and printing of documents, where critical and unique information could be authenticated [5].

Authenticating valuable documents is a research topic since a long time because of its potential market. Typical solutions are based on either physical or chemical analysis. The typical applications are cash, check or ID. However, there are also a lot of other valuable documents like certificate, contract in which the protection on its integrity is still desired. Especially in this digital age, making a fake copy is trivial by some digital ways. While there are some applications which uses the combination of security by physical means and digital means also, those are Face recognition, Iris recognition, and finger print recognition [6].

Previous work on protecting the content integrity can be categorized into two classes: watermarking-based and digital signature-based.

Currently optical watermarking presenting novel solution for authenticating printed document. Typical solution to is embedding authenticated information into the carrier which is invisible or illegible to the naked eyes but that is visualized or decoded by means of periodic phenomena, such as an absorptive grating, a lenticular screen or the sampling frequency of a copying system .The system security is guaranteed by adopting content-based key share scheme originated from visual cryptography.

Overall our proposed system has following advantages: Secure, by adopting content-based key sharing scheme (visual cryptography), the security of authentication is guaranteed by theoretic analysis, Robust, the authentication is based on global visual effect and convenient, since no digitization is required for watermark extraction, it will reduce system cost and bring the convenience to users [7].

1.1 INFORMATION HIDING IN SECURITY PRINTING

Information hiding techniques have attracted a lot of interest, because they offer a certain degree of control by the authorized document producer. Advances in digital image watermarking leads to many interesting methods to hide information in electronic documents in image forms. The information hiding parameters must be stored in a trusted central database for verification, and the information hiding and verification are usually carried out online with that trusted central database. Those methods are robust in the sense that the hidden information can still be detected on the scanned version of the printed document. Information hiding in printed documents, in principle, is very different from digital watermarking. Here, hidden images (referred to as “latent image”) embedded in a carrier screen image are invisible or illegible to the naked eye but that are visualized or decoded by means of periodic phenomena, such as an absorptive grating, a lenticular screen, or the sampling of a copying system. The term “carrier screen images” is used by many people in this field to imply the fact that the printing of documents is in the form of dot arrays, and that printed images are in the form of halftones. As such, carrier images consist of periodical arrays of screen elements, such as dots and lines, which serve as a carrier on which the encoded information is modulated [8].

The information hiding methods discussed above are effective in hiding information by constructing and modifying dot/line patterns. There are two limitations with those methods:

First, the structure of the carrier image is simply dot matrix or (straight) line gratings. This result in a limited number of different decoders, and many decoders are easily available to public. In this case, the hidden information can be easily discovered, and the word "hiding" becomes meaningless. Second, because the carrier structure is known, the encoding methods can be easily discovered by using a microscope to view and analyze the dot/line patterns. An attacker can then obtain all necessary parameters and reproduce the same without much difficulty using commercially available image processing tools [7].

1.2 OPTICAL WATERMARK

In order to overcome the two main shortcomings of the existing information hiding methods, we developed a new information hiding method, referred to as an "optical watermark"[3].

The contributions of our work on optical watermarks are as follows.

1) Technique uses phase-modulation principles [1] to provide the theoretical basis for information hiding in half tone images, with an application to security printing. This also serves as the basis for the next two contributions.

2) Technique provide generalization of the carrier structure from simple dot/line patterns to curves, and further to generic random dot patterns, so as to increase the complexity of carrier patterns, and correspondingly, increase the number of different decoders. This is equivalent to increasing the secret key space.

3) Technique proposes a new concept of a logical carrier image so that the final printed image can be a superposition of multiple logical carrier images (referred to as a watermark layer), each encoded with their own hiding information. The advantage of superposition of multiple watermark layers is that the structure of each carrier image and modulation method is not visible under microscopy and, therefore, it is extremely difficult to reproduce the same.

The basis of an optical watermark is "digital printing" [3].

This includes:

1) digital printing, where we are in the space of a higher resolution grid system, where there is either a "black/color" or "white" dot at each position;

2) any printed gray level or color images, documents, which are made of dot/line patterns;

3) dot/line patterns which are constructed on top of a high-resolution grid system. The optical watermark presented in this article is a method to "print" documents or images using specially designed "dot/line patterns" so that the latent images are hidden with a certain level of security.

2. INFORMATION HIDING BY PHASE MODULATION

Information hiding in the optical watermark is "visual information hiding." The information here is in the form of images (text, graphics, picture, etc.). After being embedded into the watermark, the visual information, or latent image, is not visible to human eyes, unless with the aid of a corresponding decoder (we call it "key" in many places). This is achieved through the low-pass filter characteristics of human eyes. It has been shown that the human visual system's contrast sensitivity varies with the spatial frequency of the signal. It has the highest sensitivity in the middle frequency range, with a sharp drop in sensitivity at high spatial frequencies, and a gentler but still obvious sensitivity loss at low frequencies. Hence, the human visual system can be approximated as a low-pass filter.

Figure 1 explains the Information Hiding by Phase Modulation. This technique establishes the mathematical framework for information hiding by using a well-known principle of modulation and the low-pass filter property of human eyes in the context of visual information hiding [1]. This serves as the basis of the optical watermark.

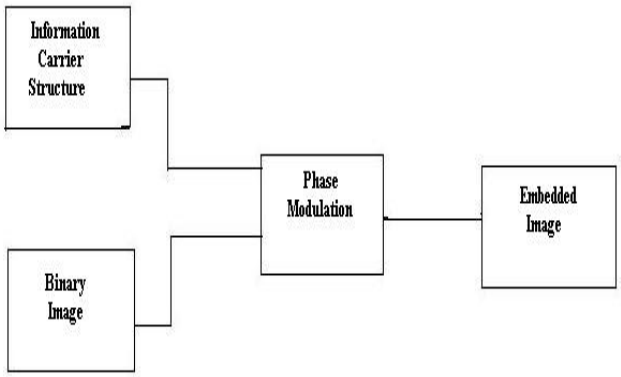

Figure 1. Embedding by Phase Modulation

The basic (or simplest) information carrier structure can be a dot array, a simple repetitive structure. In phase modulation, a binary image is embedded along either X axis or Y axis. The binary image will be modulated in the direction of x axis, by shifting the image with a half period of dot matrix in the x direction. Based on properties of the human visual system and modulation principle, the hidden information will become visible to the human eyes only when a right "key" will positioned on top of the optical watermark with the right alignment. Here, "keys" play the similar role as keys in encryption, that will to decode hidden information .The hidden information becomes visible to the human eyes only when a right "key" will positioned on top of the optical watermark with the right alignment.

2.1 BASIC INFORMATION CARRIER STRUCTURE

The basic (or simplest) information carrier structure is chosen to be a dot array, a simple repetitive structure. The dot array can be represented by a reflectance function $f_0(x,y)$ in Eq^n (1) , where T_x and T_y represent the period of the dot array in x and y directions, and D_x and D_y are the width of the dot in two directions .Figure 2 shows the Carrier Dot Array Structure implemented by using Eq^n (1).

$$F_0(x, y) = 1 - \sum_{n=-\infty}^{\infty} \Pi(x - nT_x/D_x) \sum_{n=-\infty}^{\infty} \Pi(y - nT_y / D_y) \quad \text{--Eq}^n\ (1)$$

where

$\pi(x) = \{0, \quad |x|>1/2$ is unit function

$= \{1, \quad |x|\leq 1/2$ is unit function

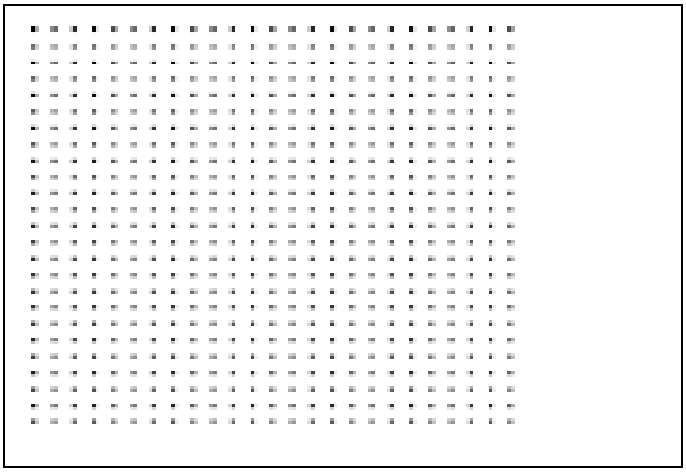

Figure 2. Carrier Dot Array Structure

2.2 PHASE MODULATION TO EMBED LATENT IMAGES INTO BASIC INFORMATION CARRIER STRUCTURE

For simplicity, we show a latent image embedding by phase modulation along either the x axis or y axis. Figure 3 and 4 is an example of such phase modulation. The first latent image, "T," is modulated in the direction of X axis (as shown in Fig 3), by shifting the "T" image with a half period of dot matrix in the x direction. While the second latent image "T" is modulated in the direction of the Y axis (as shown in Figure 4), This is done by shifting the "T" image upward with a half of period of dot matrix. As shown in the figure, the phase modulation results in visible spatial phase changes on the boundary of the latent images. In order to avoid detection of the modulation at boundaries by the human eye, those denser dots are replaced with specially designed dot patterns, which may use smaller dot

sizes or less phase shifts to achieve the similar visual effect as the other nonboundary parts.

Now let us consider the case that a binary latent image (here, it is the character "T") to be modulated on one basic information carrier structure in the axis, as shown in Figure 3. The phase-modulated carrier structure can be written as Eq^n (2). For the sake of simplicity, we let the phase shift be a half period in Eq^n (2). It can be easily generalized to the phase shift of any value

$$w(x, y) = 1-\{g(x, y) \sum_{n=-\infty}^{\infty} \Pi (x-nT_x/D_x) + [1- g(x, y)] \sum_{n=-\infty}^{\infty} \Pi (x-nT_x-(T_x/2)/D_x) \} \quad \text{-- Eq}^n\ (2)$$

we define w(x,y) as,

$$w(x, y) = g(x,y) \sum_{n=-\infty}^{\infty} \Pi (x-nT_x/D_x) + [1- g(x, y)] \sum_{n=-\infty}^{\infty} \Pi (x-nT_x-(T_x/2)/D_x) \quad \text{--Eq}^n\ (3)$$

Substitute them into Eq^n (2) and get

$$W(x,y)=1-w_1(x,y) \quad \text{--Eq}^n\ (4)$$

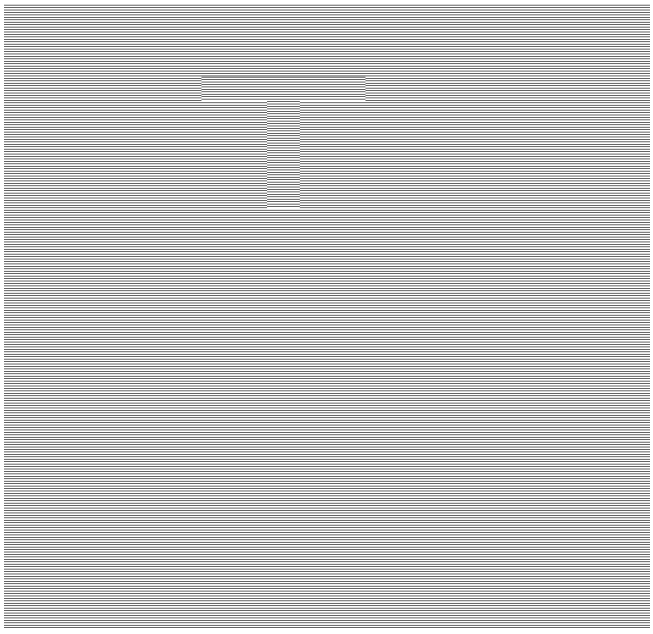

Figure 3. Modulated 'T' with respect to x-axis

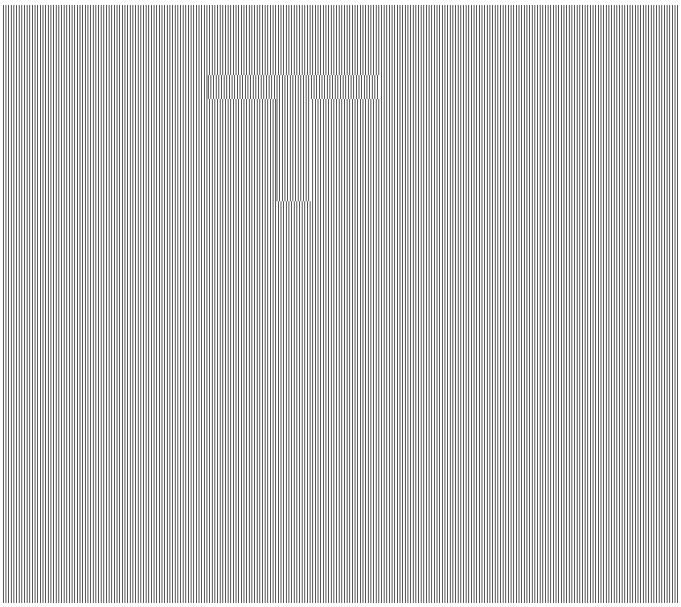

Figure 4. Modulated 'C' with respect to y-axis

2.3 DEMODULATION

Based on the fundamentals of modulation–demodulation, a latent image embedded in an information carrier structure as in Eq^n (2) can be demodulated when a set of reference line grating with the same frequency is superposed at a right angle. Now we show how demodulation is performed using a set of line gratings.

Let us use $f_r(x,y)$ to denote the reflectance function of the reference line grating, where is the Θ angle between the line grating and y axis, and $0^\circ \le \Theta \le 90^\circ$, as shown in Figure 5.

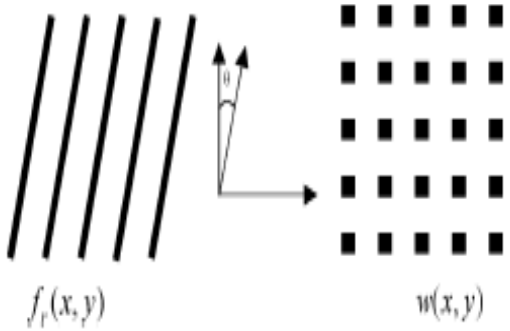

Figure 5. Reference line grating

Tr and Dr represent the period of the line grating and the width of line, respectively

$$f_r(x,y) = 1 - \sum_{n=-\infty}^{\infty} \Pi [(x \cos\theta - y \sin\theta - n T_r)/D_r]$$

The superposition of the reference line grating and the modulated carrier structure can be

represented as,

$$D(x,y) = f_r(x,y)[1-w_1(x,y)] \quad \text{-- Eq}^n.(5)$$

3. MULTIPLE-LAYERED WATERMARK STRUCTURE

The information hiding method in the previous section is in the context of a "single layer" optical watermark. It is the basic information carrier structure acting as the carrier of the information of latent images. Latent images are phase modulated on the information carrier structure, and cannot be observed by human eyes. Only with the correlative reference line gratings can the embedded latent images be demodulated and become visible to the observer. However, this information hiding method takes advantage of the low-pass filter characteristics of
human eyes. In the single-layer case, the "hidden" latent images and embedding methods can still be discovered by investigating the detailed structure of the watermark structure under a microscope.

In other words, a single-layer watermark with a simple carrier structure is not very secure because its structure is simple and is easily exposed under microscopy. Here, higher frequencies
are no longer a barrier to human observers with the aid of microscopes.

In this section, we will describe a multiple-layered optimal watermark structure, which systematically superposes multiple "single layer" optical watermark as shown in Figure 6. The superposition is not a linear operation. Therefore, it is difficult to recover individual layers without prior knowledge, while latent images modulated on those layers can be still observed using corresponding "keys." In order to achieve this goal, the information carrier structure in all layers of the "multiple layer optical watermark" should be independent of each other so that they do not interfere with each other. With that condition, the ideal demodulation of all latent images can be achieved. The term "independent" means "uncorrelated" or "orthogonal" in signal processing terms.

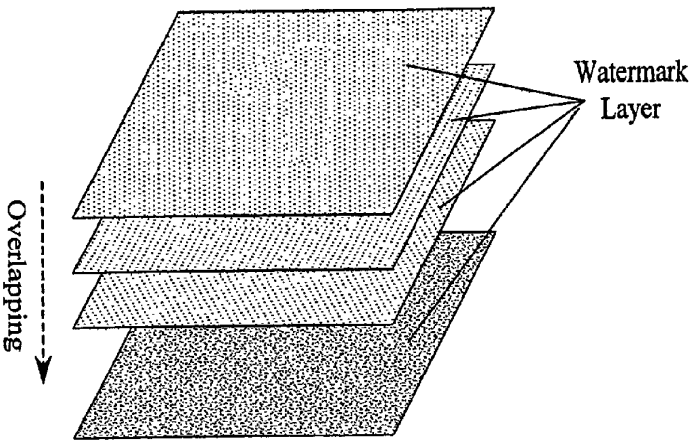

Figure 6. Super positioned watermark layer

3.1 WATERMARK LAYER

The basic information carrier structure of each watermark layer is a dot array. Let us further incorporate the orientation, and represent a watermark layer as [3],

$$L(f_u, f_v, D_u, D_v, \theta, g_u, g_v) =$$
$$1 - \{ g_u(x,y) \sum_{n=-\infty}^{\infty} \Pi (x \cos\theta + y \sin\theta - (n/f_u)/D_u) + [1-g_u(x,y)]$$
$$\sum_{n=-\infty}^{\infty} \Pi (x \cos\theta + y \sin\theta - (n/f_u) - (1/2\ f_u)/D_u) \}$$
$$\{ g_v(x,y) \sum_{n=-\infty}^{\infty} \Pi (y \cos\theta + x \sin\theta - (n/f_v)/D_v) + [1-g_v(x,y)]$$
$$\sum_{n=-\infty}^{\infty} \Pi (y \cos\theta + x \sin\theta - (n/f_v) - (1/2\ f_v)/D_v)\} \quad \text{--Eq}^n\ (6)$$

The watermark layer L (f_u, f_v, Du, Dv, θ, gu, gv) can be considered as a rotated information carrier structure that has frequency f_u along u direction and frequency f_v along v direction. The size of each dot in the watermark layer is D_u x D_v. There is an angle θ between the y axis and v direction. This angle is the orientation of the information carrier structure in each watermark layer.

3.2 SUPERPOSITION OF WATERMARK LAYER

The superposition of multiple watermark layers can be represented as the product of reflectance functions of all watermark layers [3]. Hence, the optical watermark, which is the superposition of N watermark layers, can be represented as,

$$W = 1 - \prod_{n=1}^{N} L_n (f_u, n, f_v, n, D_u, n, D_v, n, \theta_n, g_u, n, g_v, n) \quad \text{--Eq}^n (7)$$

4. SECURITY ANALYSIS OF OPTICAL WATERMARK WITH INFORMATION CARRIER STRUCTURE OF BASIC DOT ARRAYS

In the case of using a basic information carrier structure in a single-layer optical watermark, the decode key is line grating. The parameter of the key is only one–its spatial frequency. The spatial frequency range is from 380 lines per inch (LPI), the highest line screen frequency for commercial printing, to 50 LPI, the lowest spatial frequency which is able to provide enough capacity for latent image embedding. Note here that the principle of decoding is based on correlation. When the decode key and the watermark has a frequency difference, there will be a "beat frequency" in the decode result. In our context, this beat frequency will appear as moiré fringes [4]. A 10-LPI beat frequency will appear as ten strips of moiré fringes in one inch. From our empirical knowledge, a beat frequency of more than 30 LPI will eventually make the latent image unrecognizable.

Now let us consider three layers of a basic information carrier structure. Due to the superposition of three layers, it is impossible to reveal frequencies of individual layers. The superposition of multiple layers does prevent the adversaries from visual inspection of a watermark using a microscope, but it does not change the fact that the number of possible keys for each layer is still merely 11 [2].

5. IMPLEMENTATION AND RESULTS

A) Basic Dot Array Structure

Eq. (1) is used to generate the basic dot array and illustration of dot array parameters are as shown in Fig 7 , While generating this grid array the inter pixel distance tx and ty is adjusted(refer figure 8 for tx and ty inter pixel distance)

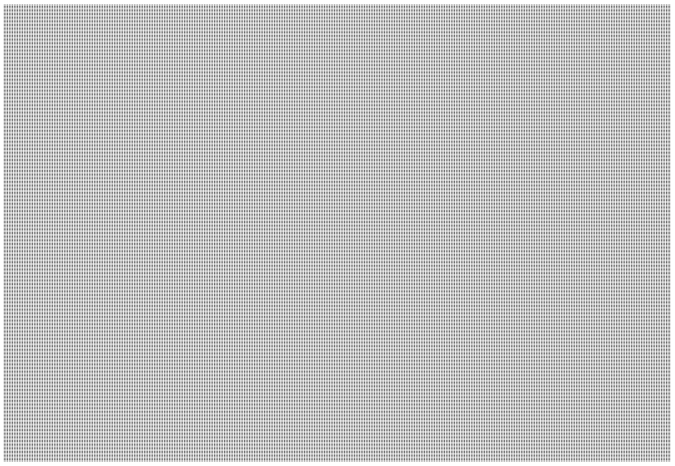

Figure 7 .Basic Dot Array Structure

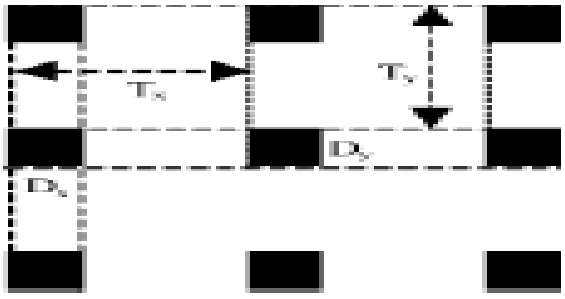

Figure 8.Inter pixel distance

B) Modulation,

Below results are obtained by using Eq^{n} (2),where carrier image is modulated with respect to Latent Image with different angle orientation.Table 1 shows the PSNR calculation of carrier Image and the modulated resulting Image.

Figure 9. Carrier Image 1)

Figure 10. Latent Image 1)

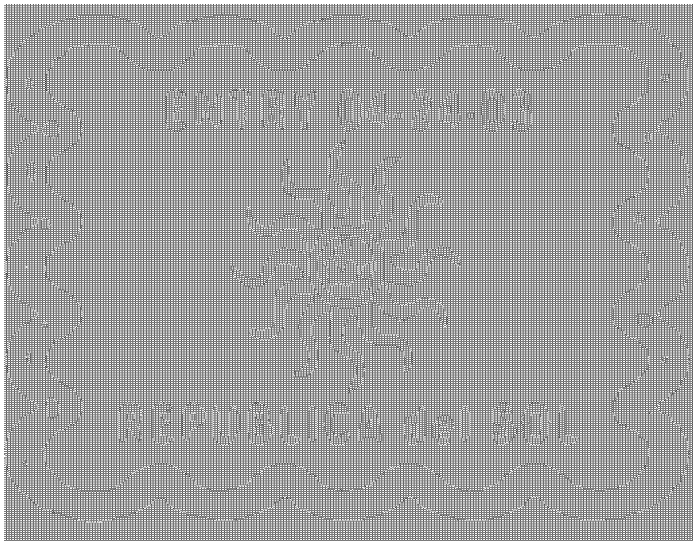

Figure 11. Result Image 1) obtained by modulation of Carrier Image 1) with respect to Latent Image 1) with 10º angle orientation.

Figure 12. Carrier Image 1)

Figure 13.Latent Image 2)

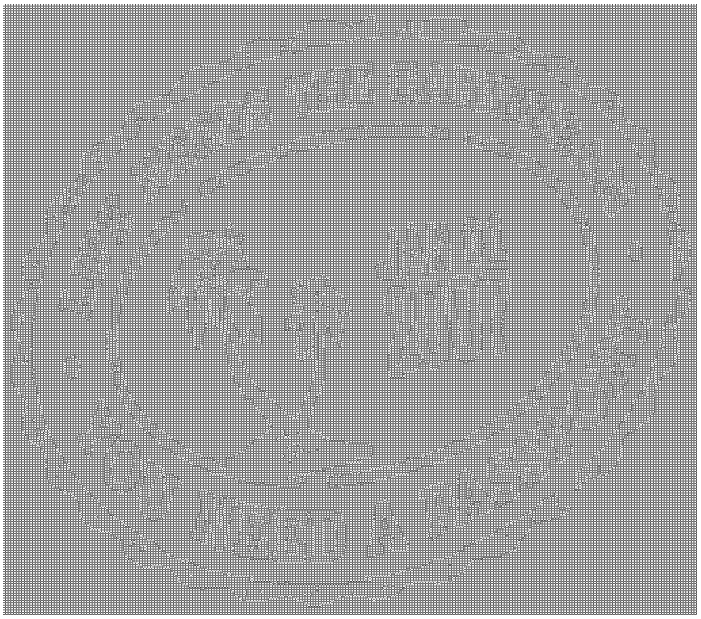

Figure 14. Result Image 2) obtained by modulation of Carrier Image 1) with respect to Latent Image 2) with 20º angle orientation.

Figure 15. Carrier Image 1)

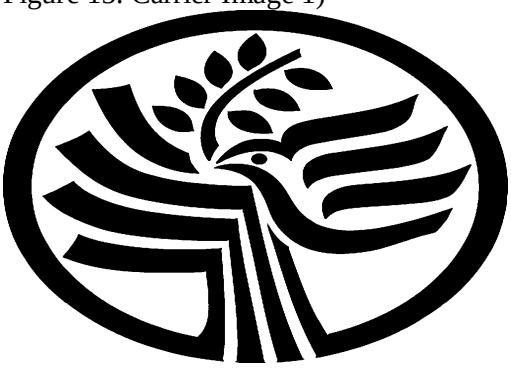

Figure 16.Latent Image 3)

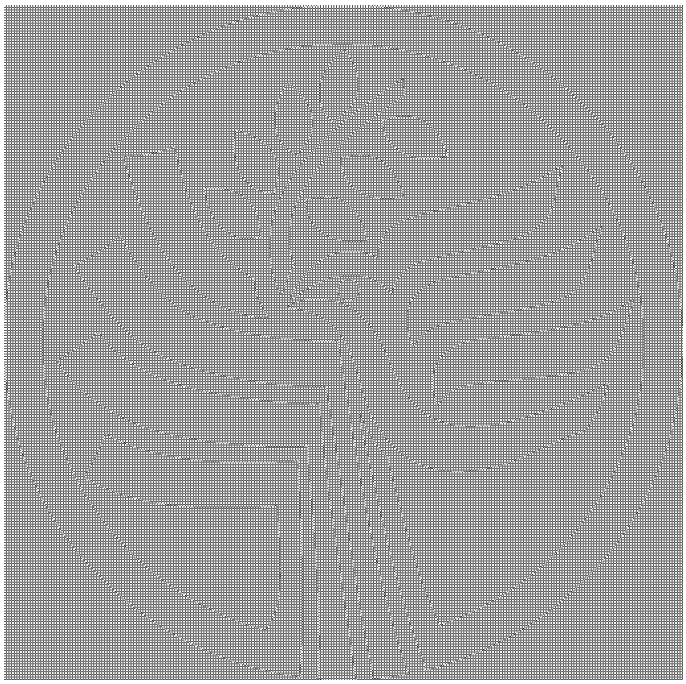

Figure 17. Result Image 3) obtained by modulation of Carrier Image 1) with respect to Latent Image 3) with 30^{o} angle orientation

Table 1.PSNR calculation of carrier Image and Latent Image.

Sr No	Carrier Image	Latent Image	Result Image	PSNR (Carrier Image and Latent Image)
1	Carrier Image 1)	Latent Image 1)	Result Image 1)	51.6025
2	Carrier Image 1)	Latent Image 2)	Result Image 2)	51.7420
3	Carrier Image 1)	Latent Image 3)	Result Image 3)	51.2889

C) Demodulation

By demodulation the information embedded in modulation can be extracted. By using Eq^{n} (5) the demodulation is obtained . Below are some results for demodulation.Table 2 provides the comparison between the Information Embedded in modulation and Extracted information obtained in demodulation in the form of PSNR.

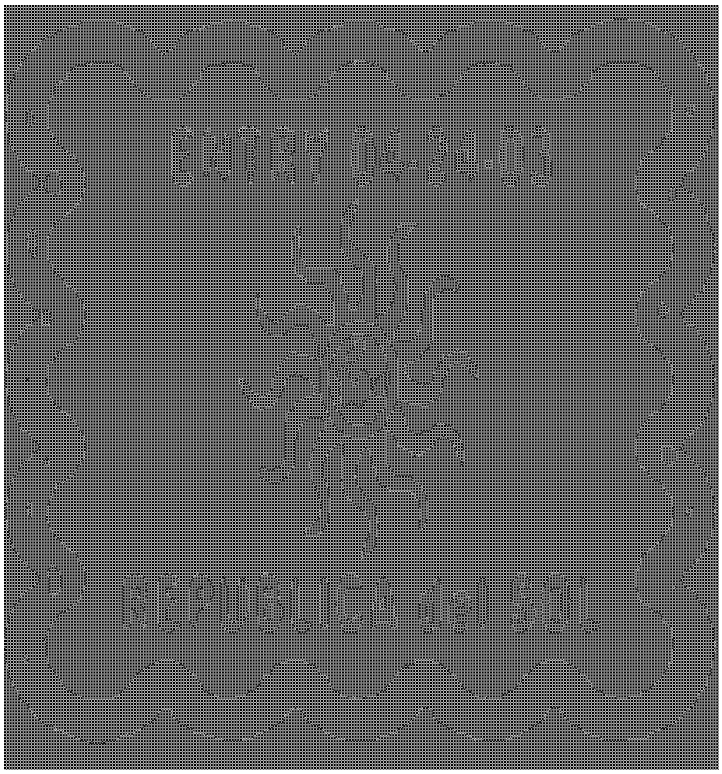

Figure 18. Demodulated result obtained from Modulated result Image 1

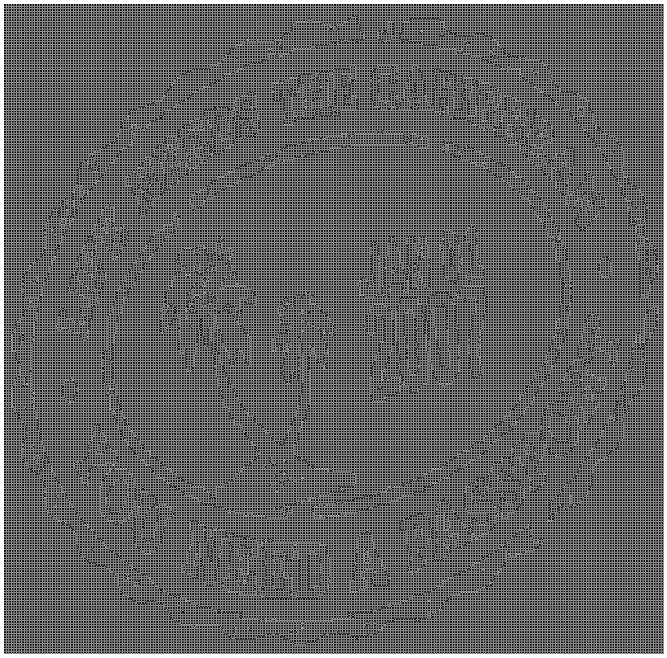

Figure 19. Demodulated result obtained from Modulated result Image 2

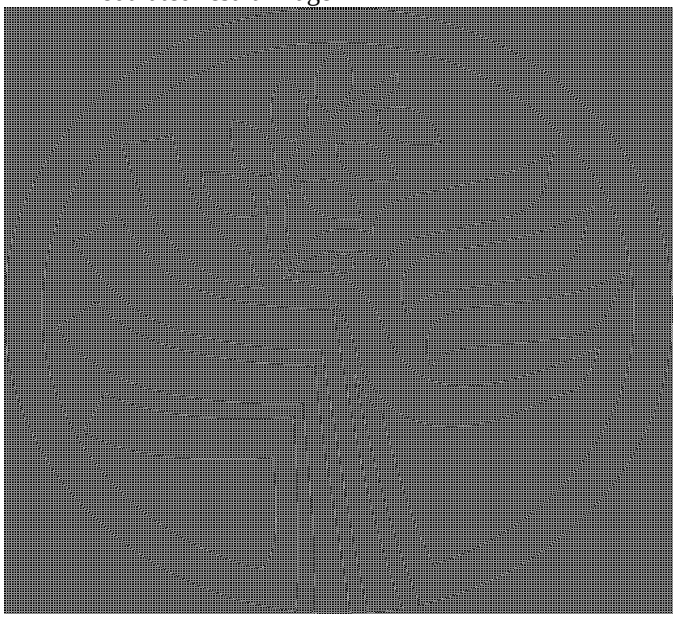

Figure 20. Demodulated result obtained from Modulated result Image 3

Sr No	Information Embedded In Modulation	Information Extracted In Demodulation	PSNR
1	Figure 10	Figure 18	50.7241
2	Figure 13	Figure 19	50.6134
3	Figure 16	Figure 20	50.9982

Table2.PSNR calculation of information embedded and extracted

D) Superposition Layer,

Below figure shows the super-positioned watermark layer. Which consists of superposition of 3 layers shown by using Eq^{n} (7) .

Figure 21. Superposition Layer obtained by Result Image 1), Result Image 2) and Result Image 3)

The experiments are carried out using Matlab7.7© and results are obtained. The Work is tested varying the values of tx and ty. The carrier image can accept latent image in the ratio 1:1 (means if carrier image is of 1024x1024 size, then it accepts the latent image of size 1024x1024).In modulation the latent image is embedded with different angle orientation. After modulation by PSNR calculation we can get idea about the distortion obtained by comparing the carrier image and modulated image. By using demodulation the latent image embedded into the carrier image ,can be extractracted. Later on, by using PSNR calculation the distortion can be obtained by comparing the original latent image and extracted latent image. And for both modulation and demodulation PSNR found near about 50 (shown in Table 1 & 2).When multiple

layer superposition is obtained then three watermark layers combined into each other to get superposition watermark layer, here each watermark layer contains different latent image with different angle orientation.

As the super positioned watermark layer is combination of three watermark layers, so it is difficult to separate these watermark layers. As a result it provides greater security towards information hiding. When proper decryption keys are applied to individual watermark layers the proper information can be extracted. The physical implementation can be seen by printing superposition layer on a paper, which contains the lots of information in it. In this way proposed system gives proper authentication towards printed documents.

Sheng Huang and Jian Kang Wu presented an optical watermarking for printed document authentication by superposition of multiple layers. The Proposed system concept is as far as similar to the concept represented by Huang and Wu [3]. The peak signal to noise ration is near about 50 for all result images, (refer table 1 and 2) which found to be good result in watermarking. The proposed system can be applied to colour images but there will be more distortion in Images.

6. CONCLUSION

An optical watermark for printed document authentication is implemented. For optical watermarking the module- Information Hiding by Phase Modulation is implemented .Visual quality of extracted image is tested using demodulation. The superposition of multiple layers effectively protects the optical watermark from reverse engineering individual watermark layers, and significantly enhances the security of the watermark. The work can be extended to improve the quality of extracted watermark.

7. ACKNOWLEDGEMENT

Authors are grateful to Head, Department of Electronics and Telecommunication, KIT'S College of Engineering and Technology, Kolhapur for technical support.

8. REFERENCES

1. H. Chabukswar, S. Shefali, "Printed Document Watermarking Using Phase Modulation", Second International Conference on Emerging Trends in Engineering and Technology, ICETET, 2009.

2. Y.F. Lu, X. Li, W. Qi, B. Yang, "A Further Study on an Optical Watermarking Scheme", ICSP Proceedings, 2008.

3. S. Huang and J.K. Wu, "Optical Watermarking for Printed Document Authentication", IEEE Trans. on Information Forensics and Security, 2, 2007.

4. I. Amidror, The Theory of the Moir´e Phenomenon: Volume II Aperiodic Layers. Kluwer, Academic Publishers, Dordrecht, The Netherlands, 2007.

5. F. Koltai and B. Adam, R.L.V. Renesse, "Enhanced optical security by using information carrier digital screening", in Optical Security and Counterfeit Deterrence Techniques V, proc. Spieis and T electronic Imaging, SPIE, 5310, 160-169, 2004.

6. D. Hsu, "Recent development of anti-counterfeiting technology in China", in Proc. Int. Conf. Advanced Anti- Counterfeiting Technologies, Beijing, China, 1-9, 2002.

7. Q.B. Sun, P.R. Feng and R. Deng, "An optical watermarking solution for authenticating printed documents", Proceedings. International Conference on Information Technology: Coding and Computing, 2001.

8. F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn, "Information hiding, a survey," Proc. IEEE, Special Issue on Protection of Multimedia Content, 87, 1062-1078, 1999.