NOVATEUR PUBLICATIONS
International Journal of Research Publications in Engineering and Technology [IJRPET]
ISSN: 2454-7875
VOLUME 3, ISSUE 8, Aug. -2017

DIGITAL IMAGE WATERMARKING USING ELLIPSE WATERMARK

SURAJ KUMAR DUBEY
Ph. D. Scholar, MATS University, Raipur, Chhattisgarh, India surajkumardubey@gmail.com

DR. A. S. ZADGAONKAR
Ex-Vice Chancellor, Dr. C. V. Raman University, Kota, Bilaspur, Chhattisgarh, India arunzad@gmail.com

ABSTRACT:

From past few decades watermarking became very crucial for digital images being transmitted over network. All the time ownership and license are great issues if someone fetches the image sent by one without any ownership seal, i.e. watermark, and uses as his own image. In this paper the basic concept of watermarking is discussed and target focus is given to ellipse watermark. As circle is a special figure of ellipse and this paper applies ellipse watermark and verifies the fact that it matches the features of circle.

KEYWORDS: Watermarking, image processing, visible watermark, invisible watermark.

I. INTRODUCTION:

Digital image processing is the study of implementing algorithms by computer to process digital images [1]. Digital image processing is much more useful and advantageous over analog image processing as it has applications in a large region of use and it uses more accurate and extended procedures for processing input images.

Digital watermarking is the method of embedding a digital watermark with any digital document or content which can be an image, text, audio, video etc. It includes impressing a digital watermark on the digital data to be transmitted from one place to another using network so that anyone who finds this data must be aware of its ownership, which is, to whom this data belongs [2].

II. WATERMARKING:

Using certain watermark and making it a part of the digital image is an application of digital image processing and is called digital image watermarking. In this a signal is embedded with digital data and becomes an integral part of it. Further any attempt to use this data incorporates embedded signal too [2]. The typical watermarking process can be illustrated as follows:

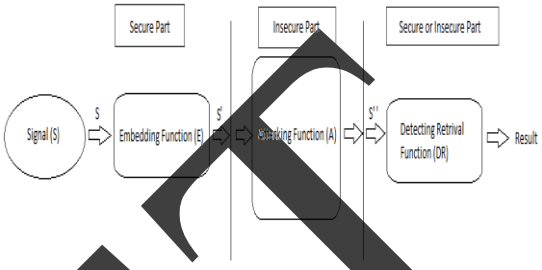


Figure 1 : Digital watermark life-cycle phases with embedding, attacking, detection and retrieval functions[2]

Here watermark is embedded with digital image/data and then it travels in the network which is in fact insecure and at the last extent watermark is extracted to ensure the authenticity of digital image/data [3][5].

Digital watermarks can be either visible or invisible. A visible watermark is visible with data and is in form of a typical text or some logo or seal. An invisible watermark cannot be viewed by nacked eyes but can be retrieved easily by certain techniques used especially for it [2].

A typical watermarking system comprises following [4]:

EMBEDDING:

In this process targeted image and proposed watermark both are submitted to the system and according to the algorithm designed for embedding process is performed and final outcome of this process is the watermarked image.

DISTRIBUTION:

Ability of owner to sell watermarked products to customer or ability to publish it over internet.

ATTACKS:

Modification by third party in watermarked image either intentionally or unintentionally. Thus watermarking method should be strong enough so that it can surpass attacking methods.

EXTRACTION:

In this process the hidden information is extracted from watermarked image.

DETECTION:

In this process accuracy of extracted watermark and quality of extracted image is examined by comparing the extracted one with the original one.

III. ELLIPSE WATERMARKING:

As on today, copyright and license should be maintained on every digital document including images without affecting the properties and view of it. An ownership seal or logo should be embedded into image in such a way that it should be viewed as a part of image itself and is supposed not to be changing the look of image markably [1].

A watermark can be of any shape and size but using an ellipse [6] shaped watermark ensures least distortion in vision of viewer who looks at the image which contains this particular watermark. Reason behind is, an ellipse watermark can be fitted anywhere in an image without affecting much to its look and feel. Degree of mixing and placing such a watermark into image decides how much it will be mixed in image evenly. Some ellipse watermarks can be as follows:

Figure 2 : Some examples of ellipse watermarks to be added to images

Efficiency and degree of embedding a watermark into an image is decided by the efficiency of embedding algorithm. The degree of embedding is directly proportional to the efficiency of embedding algorithm. Figure 3 shows normal embedding of two watermarks in an image as follows –

Figure 3 (a) : Image without any embedded watermarks

Figure 3 (b) : Example of ellipse watermarks embedding with same zoomed image

Figure 3 (a) represents the image with no watermark whereas figure 3 (b) shows image with four visible watermarks, among which watermark 1 and watermark 4 are properly differentiable from picture, but watermark 2 is more indifferentiable and watermark 3 is the most indifferentiable amongst all. It can be said that watermark 2 and watermark 3 of figure 3 (b) are sized and placed by more efficient algorithms than algorithms used to place watermark 1 and watermark 4.

Figure 4 also shows watermarking using a more efficient algorithm -

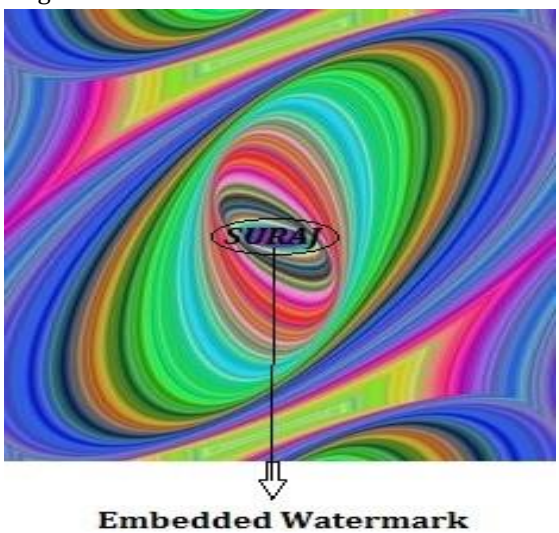


Figure 4 : Example of extended embedding of ellipse watermark with an image which is almost non-differentiable

It can be seen in figure 4 that the watermark gives the feel of being a part of image. In this image, the watermark looks like a part of image itself but size of it makes it bit distinguishable. If more efficient algorithm is used then it will be able to decide the size of watermark, position of it in image and its dimensions in image also.

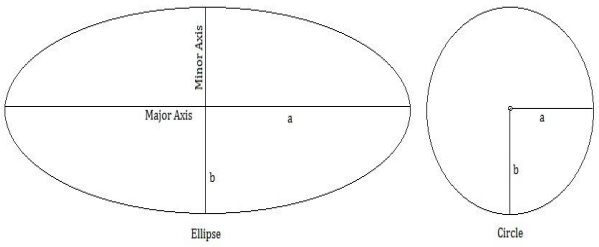
The second phase is that if image is being attacked and third party uses some algorithm to remove watermarks from it, then a way to overcome this is to use watermarks more times so that removal process should be proven ineffective in removing all the watermarks embedded with image [4]. Another way to bypass watermark removal by third party is to design such watermarks those are rarely differentiable from image and to embed them on such portions of image where they are almost indistinguishable [4].

Advantages of using ellipse watermarks are as follows –

- They are in such a shape which can be embedded easily at any coordinate position of an image.
- Though being visible watermarks, they can be intermixed in an image such that viewer can't distinguish them from image.
- They need lesser time in formation, formatting and embedding as compare to linear, rectangular, square and other shaped watermarks.
- Distribution of them is widely accepted and standardized because almost all universal organizations have included it as proper license shape.
- Much simpler procedures are needed to extract them from image whereas other shaped watermarks need more complex procedures in the process of extraction.
- Detection process has lesser time complexity in case of ellipse watermarks but other shapes take more time in detection.

IV. ELLIPSE AND CIRCLE WATERMARKING:

As it is known that the basic difference [7] between a circle and ellipse is that circle has all the points on its boundary equidistant from its center but in case of ellipse points on its boundary are not equidistant as shown in figure 5 –



a≠b a=b

Figure 5 : Illustration of both the closed shapes, i.e., Ellipse and Circle

It can be seen clearly from the figure above that that single difference between these two shapes is that in ellipse a≠b but in circle a=b, where a and b are distances of two different points on perimeter from center of shape. Both the shapes can be used for watermarking and can easily be embedded into image. Selection depends on the pattern contained by image so that one of these two shapes can be used. As it is known that circle is a special figure of ellipse and if a circle is pressed by putting it between two parallel surfaces then it becomes an ellipse without any changes in its total area and circumference.

According to the requirement and suite, one of these shapes can be used for watermarking and thus need of a process arises which can automatically search portions of image to embed watermark with and decide shape from an ellipse and a circle with decision of its size too.

V. COMPARISON OF BINARY CONVERSIONS OF IMAGES WITH & WITHOUT WATERMARKS:

Here images given in figure 3(a) and 3(b) represent image with no watermark and image with watermarks respectively. These images are converted into binary format. Binary conversions of figure 3(a) and 3(b) are as follows –

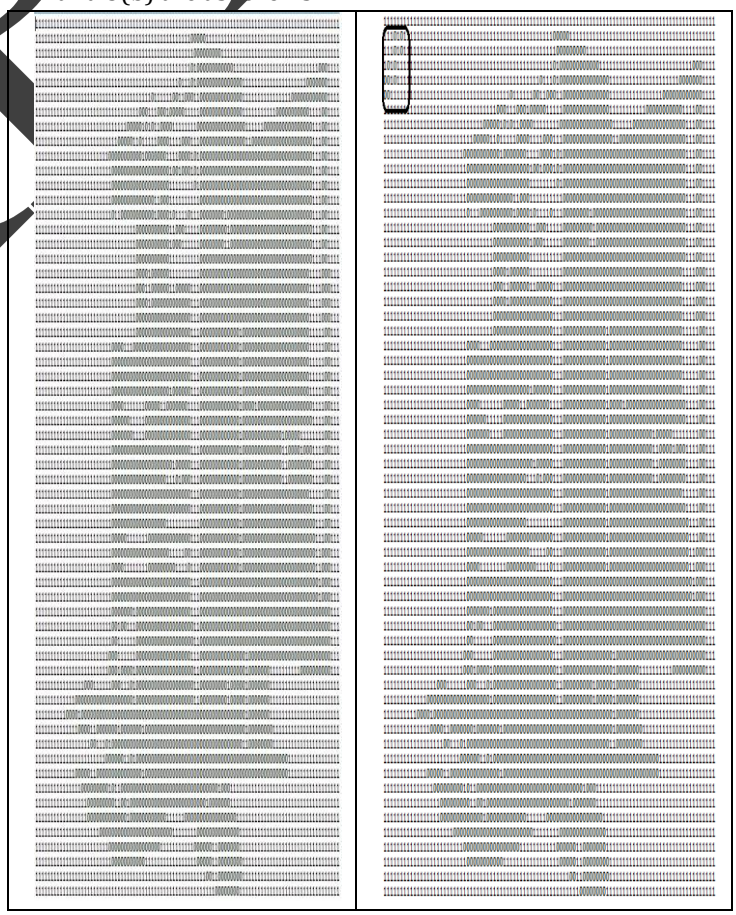


Figure 6 : Binary representations of images 3(a)-left and 3(b)-right [8]

In figure 6, two binary images are represented. First image at left is the binary conversion of figure 3(a), i.e., image without watermarks. Second image at right is the binary conversion of figure 3(b), i.e., image with watermarks. Binary conversions of these images are not only different in combinations of 0s and 1s but their visualizations also show differences which can be easily seen by nacked eyes too. But the difference in binary forms of images is not seen in view in the same way as of normal images. Because binary images are constructed in form of matrix and it again consists of rows. Therefore same pattern generation is not found in binary images obtained from normal images. This difference can be measured digitally also and this differentiation is shown in this paper in figure 7. Difference occurred in binary representation of image 3(b) depicted in right side in figure 6 from binary representation of image 3(a) is enclosed in a box.

Figure 7 also contains two binary images. Binary image on left represents the image with no watermarks and binary image on right represents image with watermarks. Differentiation summary is given at top and bottom of figure 7.

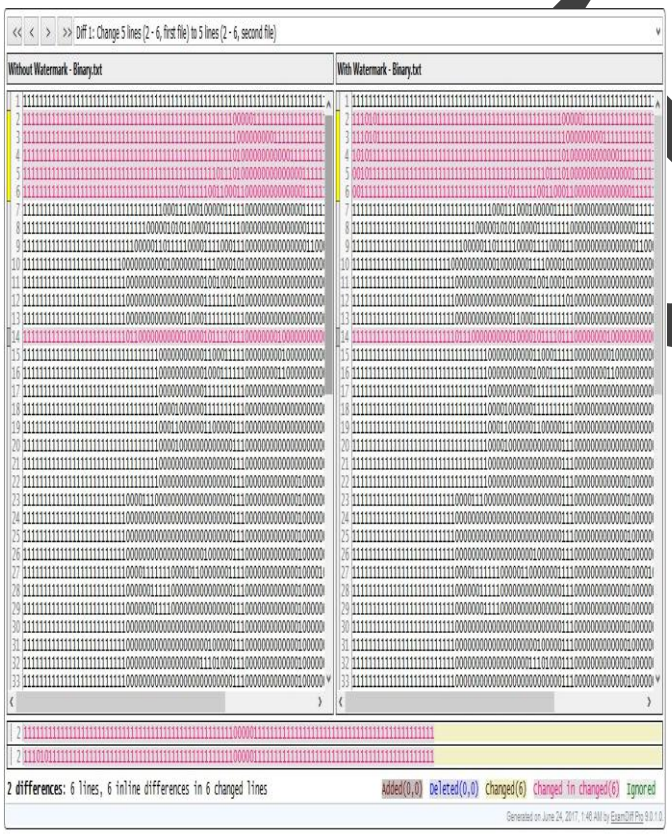


Figure 7 : Comparing binary images shown in figure 6 [9]

Figure 8 contains 2 very basic images. Image on the left has no watermark embedded whereas image on the right has embedded watermark.

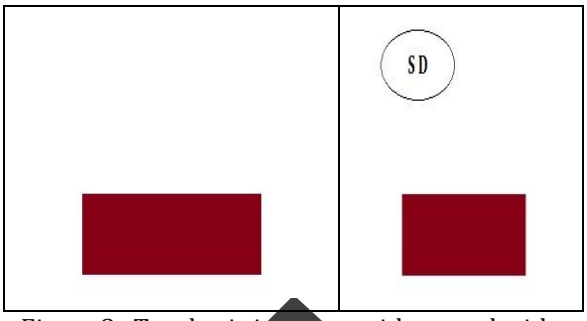


Figure 8 : Two basic images – without and with watermark on left and right respectively

Binary representations of these two images are depicted in figure 9. Left one is binary representation of left image of figure 8 and right one is binary representation of right image of figure 8. Difference occurred in right image is enclosed in a box

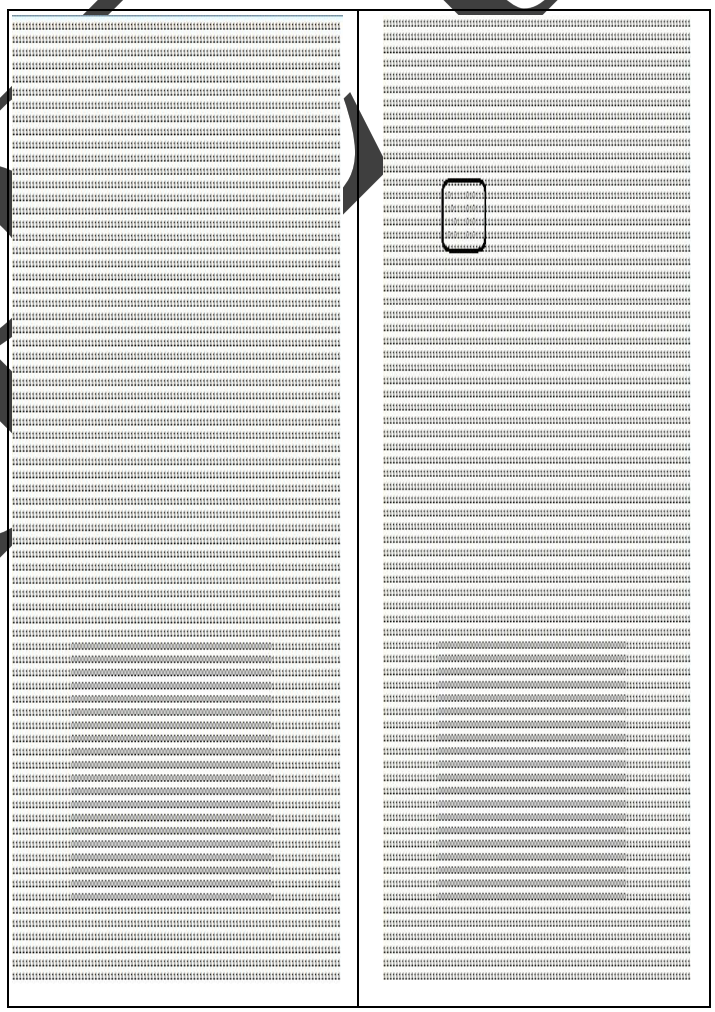


Figure 9 : Comparing binary images shown in figure 8 [8]

Even if digital policies for erasing ellipse watermark are used, then also an ellipse watermark is not erased completely. This is one the salient features of ellipse watermarks that they cannot be erased completely. Such an example is depicted in figure 10 which shows the effort put to erase ellipse watermark

shown in right side of figure 8. Figure 11 shows the binary equivalent of image shown in figure 10. Binary image depicted in figure 11 contains remaining watermark only, can be distinguished from binary representation depicted in right side of figure 9 which contains complete watermark.

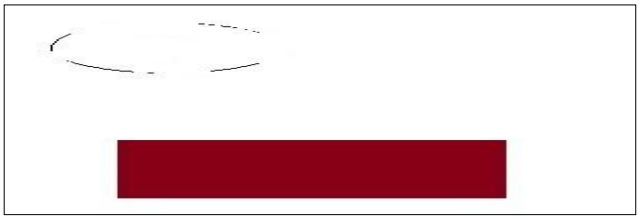


Figure 10 : Image after putting efforts to erase watermark referenced from figure 8

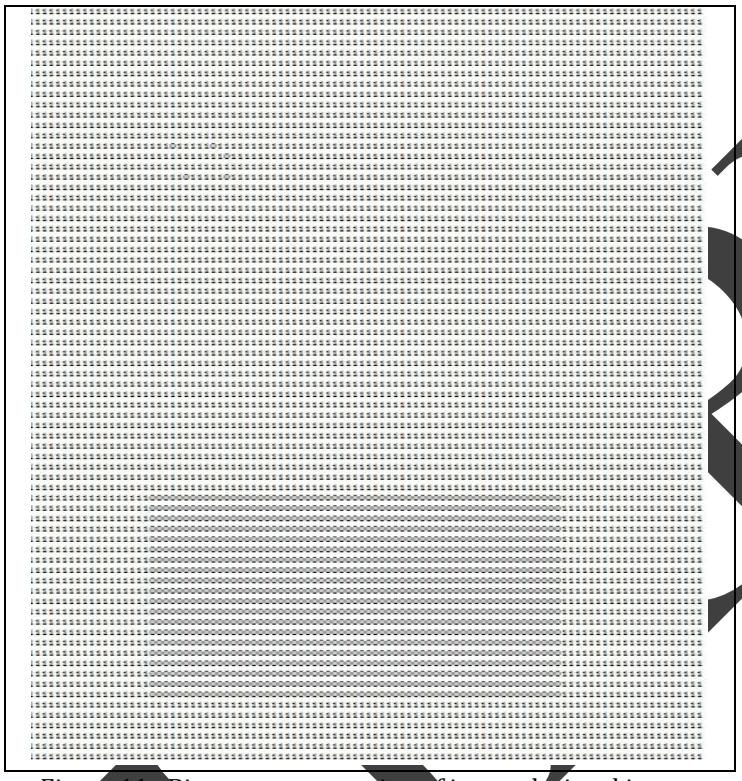


Figure 11 : Binary representation of image depicted in figure 10 [8]

Figure 12 shows the comparison of pieces of binary images from figure 9's right side containing complete watermark and from figure 11 containing partly impressed watermark. This shows only region of binary images from figures mentioned above where watermark is impressed.

10111110101 11011110101 11101110101 10101110101	101111101111 111111111011 111111111111 111011111011

Figure 12 : Segments of complete watermark and partial watermark from figure 9 and 11 respectively

Same concept is used in example ahead. An image is taken and is shown in figure 13(a) which has no watermark. Then a watermark is added in next image shown in figure 13(b). Image in figure 13(c) shows the image after attempt to remove watermark. Figure 14 shows their binary representations where figure 14(a) is binary representation of figure 13(a), figure 14(b) is binary representation of figure 13(b) and figure 14(c) is binary representation of figure 13(c).

Figure 13 : (a)Image without watermark (b)Image with watermark (c)Image after attempt to erase watermark

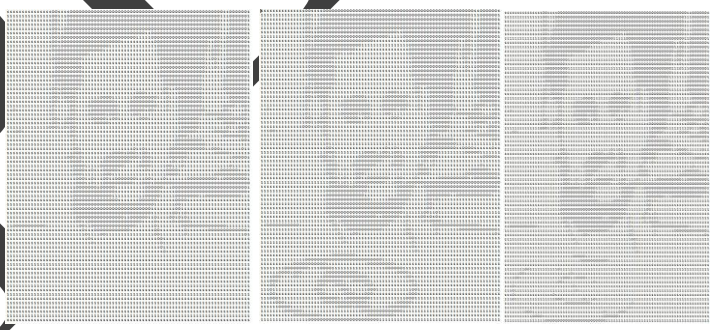


Figure 14 : (a)Binary form of 13(a), (b) Binary form of 13(b), (c) Binary form of 13(c) [8]

Same concept is implemented in next example with a difference that it contains watermark from one end to another of image diagonally and this is illustrated in figure 15. Figure 15(a) contains no watermark. Figure 15(b) contains watermark from one end to another diagonally. Figure 15(c) is representing the image after erasing 95% of watermark.

Figure 16 contains binary equivalents of images

Figure 15 : (a)Image without watermark (b)Image with watermark (c)Image after attempt to erase watermark

Figure 16 : (a)Binary form of 15(a), (b) Binary form of 15(b), (c) Binary form of 15(c) [8]

Same concept is implemented in next example with a difference that it contains watermark from one end to another of image diagonally with cross and this is illustrated in figure 17. Figure 17(a) contains watermark from one end to another diagonally with cross. Figure 17(b) is representing the image after erasing watermark and left 7 point .

Figure 18 contains binary equivalents of images illustrated in figure 17 in sequence. Figure 18(a) represents binary of 17(a) and. The binary pattern of left portion of watermark of 17(b) is enclosed in an ellipse justto show its presence in 18(b).

Figure 17 : (a)Image with watermark , 17 : (b)Image after attempt to erase watermarks

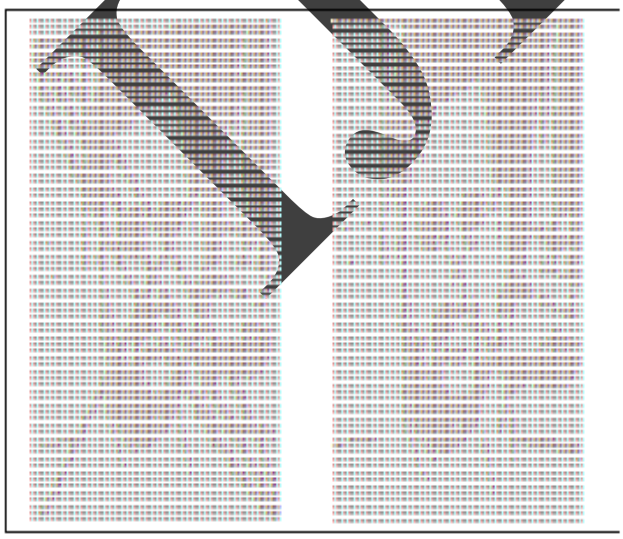


Figure 18 : (a)Binary form of 17(a), 18 : (b) Binary form of 17(b)

VI. CONCLUSION:

Digital image watermarking is still very crucial for owners to mark their copyright or license on image. Best way is to use visible watermarks but in such a way that they should not be easily distinguishable because of their properties. For the same certain algorithms are required to be introduced and such implementations are needed to identify the portions of image to embed such watermarks and best provisions are using either an ellipse or a circle.

REFERENCES:

1) https://en.wikipedia.org/wiki/Digital_image_processing
2) Suraj Kumar Dubey and Vivek Chandra, *"Steganography , Cryptography and Watermarking : A Review"*, IJIRSET, Vol. 6, Issue 2, February 2017, ISSN(Online) – 2319-8753, ISSN(Print) – 2347-6710, Page: 2595-2599.
3) Schneier, Bruce., "*Applied cryptography: protocols, algorithms, and source code in C",* John Wiley & Sons, 2007.
4) Seyed Mojtaba Mousavi, Alireza Naghsh, and S. A. R. Abu-Bakar, *"Watermarking Techniques used in Medical Images : a Survey"*, J Digit Imaging. 2014 Dec; 27(6): 714–729, Published online 2014 May 29. doi: 10.1007/s10278-014-9700-5.(https://www.ncbi. nlm.nih. gov /pmc/articles/PMC4391065/).
5) Suraj Kumar Dubey and Vivek Chandra, *"Watermarking and Cryptography in Transform Domain"*, IJTRD (www.ijtrd.com), Vol. 4(I), Jan-Feb 2017, ISSN – 2394-9333, Page: 486-488.
6) Baisa L. Gunjal and Suresh N. Mali, "*ROI Based Embedded Watermarking of Medical Images for Secured Communication in Telemedicine*", International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:6, No:8, 2012, scholar.waset.org/1999.4/4309, page: 997-1002.
7) http://conic-sabeel.weebly.com/the-similarities differences- between- all-types-of-conics.html
8) http://www.dcode.fr/binary-image
9) https://www.diffnow.com/