Open Access **Baghdad Science Journal** **P-ISSN: 2078-8665**
Published Online First: February, 2023 **2023, 20(5): 1797-1807** **E-ISSN: 2411-7986**

DOI: https://dx.doi.org/10.21123/bsj.2023.7168

Watermark Based on Singular Value Decomposition

***Ali Abdulazeez Mohammed Baqer Qazzaz*[1*]** ***Neamah Enad Kadhim*[2]**

[1]Faculty of Education, University of Kufa, Najaf, Iraq
[2] Department of Computer Sciences, College of Science for Women, University of Baghdad, Baghdad, Iraq
*Corresponding author: alia.qazzaz@uokufa.edu.iq
E-mail addresses: neimaek_comp@csw.uobaghdad.edu.iq

Received 9/3/2022, Revised 13/9/2022, Accepted 14/9/2022, Published Online First 20/2/2023, Published 1/10/2023

Abstract:

Watermarking operation can be defined as a process of embedding special wanted and reversible information in important secure files to protect the ownership or information of the wanted cover file based on the proposed singular value decomposition (SVD) watermark. The proposed method for digital watermark has very huge domain for constructing final number and this mean protecting watermark from conflict. The cover file is the important image need to be protected. A hidden watermark is a unique number extracted from the cover file by performing proposed related and successive operations, starting by dividing the original image into four various parts with unequal size. Each part of these four treated as a separate matrix and applying SVD on it, the diagonal matrix is selected to determine its norm. The four norms will be processed to produce one unique number used as a watermark and this number can be developed in future by exploiting some other features in constructing watermark number other than SVD process to construct two watermark numbers, each one of them owned special methodology, for avoiding some challenges and changings in the transformation process.

Keywords: Cover, Norm, Ownership, Singular value decomposition, Watermark.

Introduction:

Watermarking is an operation for hiding special and wanted information in a carrier to protect the ownership of the carrier file, watermarks information in the image is hidden in more significant and important regions of the image and must be not lost by some simple processes like compression . The main purpose of the watermarking process is to prevent illegal claiming of having a product. In other words, the main goal of the watermarking process is to hide a message (W) in some image, audio, or video (cover) data file (I), to obtain a new data file (I') as illustrated in Fig. 1. Virtually watermarked image indistinguishable from (I), in such a way that the third person cannot remove or replace (W) in (I'), this means that the purpose of this operation is to hide a suitable message in such a way to perform one-to-many communications [2]. Watermarking methods need to be very robust against the attempts of removing or modifying the hidden information[1].

Some famous applications of this technique are to provide a guide to the ownership of the protected digital media by hiding a proving about copyright statements into audio, video, or image digital products. Digital watermarking may be used for many applications like

- Automatic tracking of copy-write material on the web.
- Fingerprinting applications.
- Copyright protection.
- Secret communication.
- Authentication.
- Robust information Hiding [3].

Watermarking emerged as a leading process to solve some important problems (like the above). All types of information can be used in watermarking techniques such as images, text, audio, video, 3D models, …essentially, the inputs to the watermark project are the designed watermark, the cover file media, and a secret key (or keys) to perform watermark process, while the output is watermarked information. Fig. 1 shows the basic scheme for watermark technique [4].

Baghdad Science Journal
2023, 20(5): 1797-1807
P-ISSN: 2078-8665
E-ISSN: 2411-7986

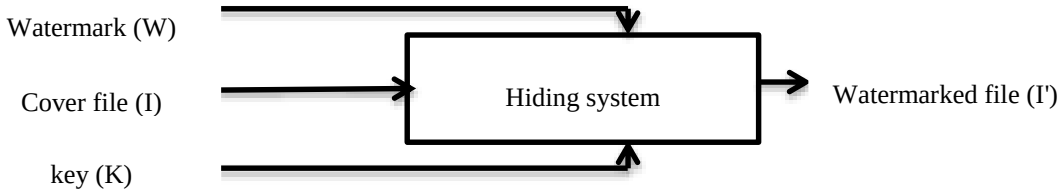


Figure 1. The system of watermark

The requirements of watermarking technique are

- Security: this requirement differs slightly depending on the application. The security of watermarking technique means that the embedding watermark should be very difficult to alter or remove without visible effecting or damaging in the cover file [5].
- Imperceptibility: this means that no sensible alter between the watermarked media and the original file will occur.
- Capacity: The amount of data that can be hiding into a cover signal.
- Robustness: The capability of the watermark signal to survive signal manipulations. A watermark must resist the attacks and some processing performed on a signal that is happened during the period of transforming in a communication channel [2].

Watermarking processes can be classified depending on some affected factors as illustrated in Fig. 2.

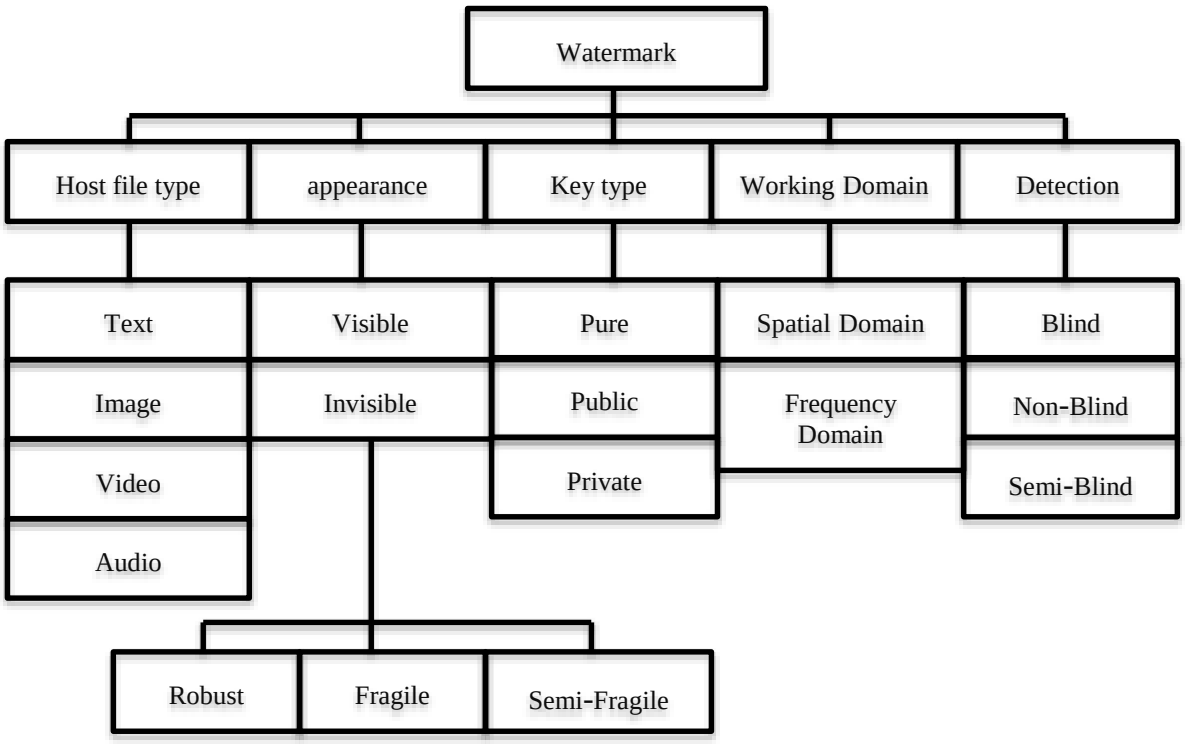


Figure 2. Taxonomy of watermark

From the human perception side, watermarks techniques are divided into the following kinds:

1- Visible.
2- Invisible.

In the visible watermark, the designer makes light modifications to the cover image where the image still completely visible, so the watermark aspect appears in the cover image, even if an image is printed or scanned [6]. The visible watermark ordinary makes the pixels of the watermark either lighter or darker than the other surrounding pixels. The watermark is covering a large and enough number of pixels in the cover image with making sure that the original cover image is visible with a good degree of clarity, so the watermark cannot be manipulated or removed as illustrated in Fig. 3.

Figure 3. Visible watermark

The invisible watermark cannot be detected or seen by the human eye and this process is implemented by changing some certain pixel values as illustrated in Fig. 4. The strength of the invisible watermark depends on some affecting factors and the most important one is that the image quality is not degraded [3]. If a digital image has an invisible watermark printed, and then scanned, the watermark has normally been removed [7].

The invisible watermarks can be classified into three kinds from the robustness side:

Figure 4. Invisible watermark

1- Robust Watermark.
2- Fragile Watermark.
3- Semi-Fragile Watermark.

The first kind of watermark "robust watermark" is proposed for some applications like copyright, protection against copy, content tracking, and monitoring the broadcast, where hiding watermark is very difficult to remove. The robust watermark kind must be a permanent and inseparable part of the cover or original signal [8]. Despite no watermark is indestructible, a technique may be robust if the amount of changes wanted for removing the watermark makes the original file damaged and therefore without interest [5]. According to previous reasons the watermark should be embedded in selected parts of the file where any change or removal for it would be easily discovered. There are two types of this kind of watermarks mainly:

A- Fingerprinting: in this type of watermark, a unique mark of the identifier represents one customer who owned the file will be hidden and therefore, allows using this file [1]. The copyright owner of the digital file uses the fingerprint for defining the person that violated the license agreement by providing a copy of the file [9]. Ideally fingerprinting should be used but for mass production of CDs, DVDs, etc. it is not possible to give each disk a dedicated fingerprint.

B- Watermarks: they define person/(s) who own(s) the copyright of the special file, instead of the customer-like robust watermark. Watermarks help in preventing and detecting persons that have an illegal copy. Watermarks will be hidden to prevent operations like detecting and removing the signal [10].

Fragile watermarks are not designed as robust against detection and removal. On the contrary, a fragile watermark is designed to be destroyed because of any simple slightest change, alteration, or modification performing to the watermarked file. While watermarking requires robustness to image manipulation, data hiding requires that there is very little visible distortion in the host image [11].

This process is useful for the authentication of some applications, where the purpose is to provide confidence that a signal originated from a known source, and a signal has not been altered as illustrated in Fig. 5 [12].

Figure 5. Fragile watermark

The acceptability of a watermarked file can be obtained by using the watermark detector. If the detector is successfully found and detected the embedding watermark, both sides of the signal are authenticated. The integrity of the file is authenticated because any altering process will damage or destroy the hided fragile watermark. If the watermark is not detected in the correct form, then either the file will not be produced from the source or the entire file will be altered in some stations [5].

One of the important disadvantages of fragile watermarking is that it may be too sensitive for some applications like lossy compression technique applied on a watermarked image, then the detector of the fragile watermark will report a tampered in the watermarked file even though the compressed image appears with large degree nearly the same as the watermarked image [3].

A semi-fragile technique merges the properties of robust and fragile techniques. Similar to robust technique because of its capability of resisting changes performed to the output watermarked file, like adding some information in lossy compression, and similar to fragile technique because of its capability of detecting places in the image that have been essentially altered [2].

Another classification depends on the detection design feature in the watermarking algorithm: whether they are formed to do blind or non-blind detection. Blind detection is the ability of the technique to detect and solve the watermark without altering the original content. Semi blind method requires some additional information for extraction of the embedding watermark [6]. The non-blind watermarking techniques are more robust than blind watermarking systems due to the availability of the original cover file at the time of detection. However, blind watermarking systems are more popular then most important characteristics for these methods are the ability to recover without distortion of the actual cover image, and the tamper proofing added with authentication. The purpose of integrity and authentication of the cover watermark application is to find and localize a place of tampering [13].

For blind watermarking techniques new algorithms provide a new solution for applying SVD as the embedding using secret sharing schema (SSS) [14].

Singular Value Decomposition (SVD)

One of the most interesting algorithms used by the researchers is singular value decomposition (SVD), which is a numerical analysis algorithm developed for a variety of applications. From the viewpoint of image-processing applications, SVD

includes two properties related to its singular value of an image: 1) stability when adding a small perturbation to an image and 2) intrinsic algebraic image properties.

The SVD of an array such as (B) is the division of array (B) into three special matrices UDV^T (with production operation between them) where the columns of arrays (U and V) are orthonormal and the array (D) is diagonal consist of positive and real values as illustrated in Fig. 6 [15].

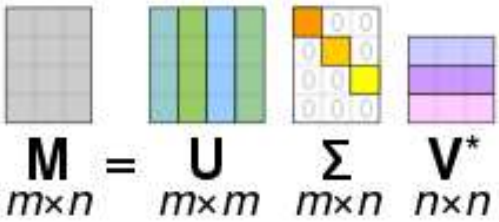


Figure 6. Singular value decomposition of matrix B (n×d)

The SVD is important and useful in many operations like

1- The data array (B) is close to an array of low rank and it is used in deciding low-rank array which is accepted as a good approximation to the original data array, this means, from the singular value decomposition of an array (B), the matrix (B) of selected rank like (k) is a good approximation for array (B).
2- SVD is defined for all arrays (rectangular or square) unlike the more commonly used spectral decomposition[8]. The columns of the array (V) in the SVD represent the right singular vector of (B), always form an orthogonal set with no conditions on (B), and the columns of (U) represent the left singular vector of (B) and also considered orthogonal set. the inverse of (B) is ($V D^{-1}U^T$), where (U) orthogonal array with size (m × m) and its columns represent the eigenvectors of (BB^T), (V) is also an orthogonal array with size (n × n) and its columns represent the eigenvectors of (B^TB), and (D) is a diagonal array with size (m × n) and form of

$$S = \begin{pmatrix} \sigma_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \ddots & 0 & 0 & 0 & 0 \\ 0 & 0 & \sigma_r & 0 & 0 & 0 \\ 0 & 0 & 0 & \ddots & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

with $\sigma_1 > \sigma_2 > \cdots > \sigma_r > 0$ and r = rank(B). and $\sigma_1, \sigma_2, \ldots, \sigma_r$ are the square roots ($\sqrt[2]{B^TB}$) of the (B^TB), and known as the singular values (SV) of (B) [15].

Related Work

1- Mr.P.B.Khatkale, et. al. in[16] suggested a technique for watermarking by hiding information in input images by exploiting the insensible changes to the human eye but they are calculated by a computer program and therefore they are reversible. Generally, the watermark is a guide to identify the owner of a media file. The positions in which the watermark is embedded are decided by using a suitable secret key, to prevent possible hackers from easily changing or removing the hidden watermark. Furthermore, the watermark technique should be recoverable without any altering in the watermark image. Possible hackers used some operations in a watermarked image like filtering compression and cropping. The main application of the watermark process is copyright protection of digital media.
2- Prof. S. C. Tamane, et. al. in [9] presented new hiding techniques for developing security requirement and satisfying the requirements of robustness, imperceptibility, capacity (data hiding rate), and security of the message to keep digital file work in correct fashion for the owner of the work and work reliably for the customer of the file. Some searches selected significant and important parts of the image, for modifying to hide the information in a robust and reliable place in a perfect way. This led to making watermarking techniques working in the frequency domain instead of special ones. The wavelet transform has many advantages over DCT transform for example that this transform can be used in compression operation as well as watermarking process. Therefore it is very true to consider the wavelet domain in embedding processes for watermarking techniques.
3- Kunal D Megha, et. al. in [13] introduced the idea of exploiting the topography of the digital watermark by performing steps like converting input image with (RGB) model to (YIQ) model, applying (Discrete Wavelet Transform) on (I) - matrix, calculate coefficients of (WT), taking grayscale watermark image for hiding, applying (DCT) on the watermark gray image, inserting (DCT) coefficients into (DWT) coefficients, applying inverse (DWT) and for extracting watermark performing previous operations but in reverse order. Results of this technique are examined for all bands of (RGB) and (YIQ) models. Performance metrics are performed for measuring the efficiency of the explained technique, robustness feature is measured by using the (PSNR) metric, and we know that a

bigger value of (PSNR) means the best quality in results.

4- Rajitha and shivendra [17] introduced DWT-SVD based self-authentication image scheme for telemedicine application. In this scheme the first phase is pre-processing, the second is self-authentication, and the final step is tamper detection.

Proposed System

The proposed or suggested system consists of many steps for extracting a unique watermark number for each image and then hiding this unique number into a suitably protected region in the input image and these steps can be illustrated in Fig. 7.

Each step of the suggested system can be illustrated as follows

1- Dividing input image into four non-similar parts:

This process can be applied depending on some extracted suitable keys from the input image, these keys can be calculated by applying the following equations

$$PVB = round(\frac{FPV}{NGL} \times W) \quad \ldots 1$$

$$PHB = round(\frac{SPV}{NGL} \times H) \quad \ldots 2$$

Where

PVB represents the position of the vertical boundary.

PHB represents the position of the horizontal boundary.

FPV represents the value of the first pixel in the last row in the input image.

SPV represents the value of the second pixel in the last row in the input image.

NGL represents the total levels of gray color in the input images.

W, H represents the width and height of the input image.

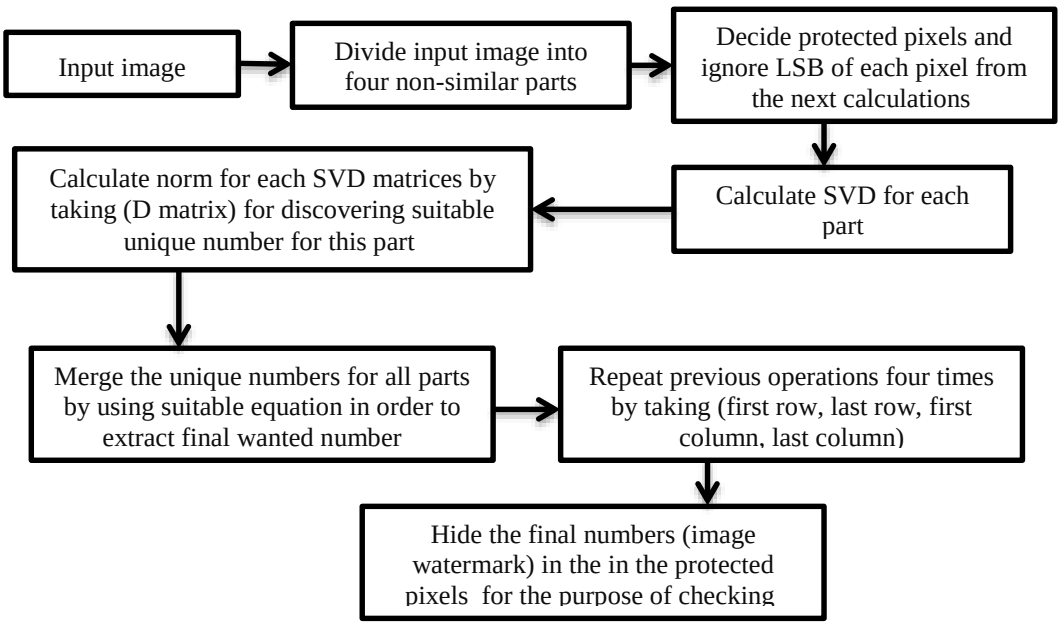


Figure 7. Block diagram of the proposed system

These two equations ensure non-equality between the final four parts depending on simple features extracted from the input image as illustrated in the following example for matrix A and Fig. 8.

2	1	2	3	0	7	4	4	1
4	7	7	6	5	4	5	4	3
1	2	7	3	4	2	2	2	3
7	4	3	5	4	7	2	4	4
6	5	7	2	6	5	4	3	5
4	2	1	7	4	1	5	2	4
3	2	5	1	3	1	2	3	2

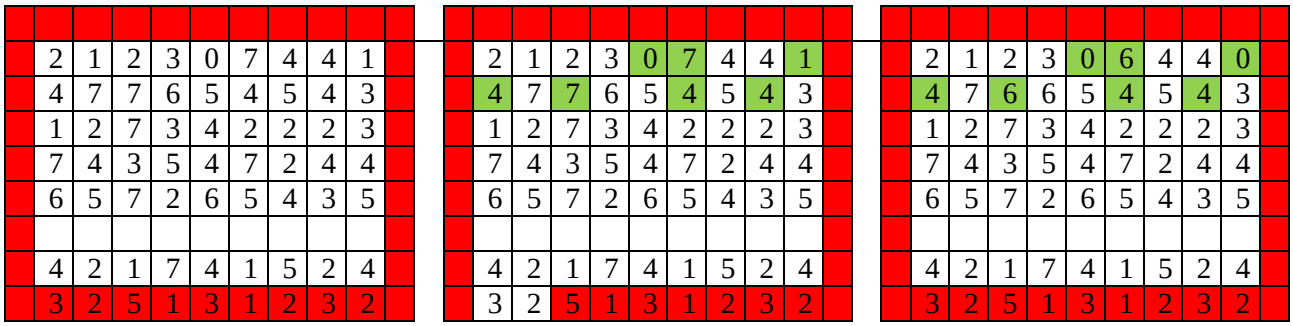
Figure 8. Example to illustrate dividing image into four parts

$$PVB = round(\frac{FPV}{NGL} \times W) = \frac{3}{8} \times 9 = \frac{27}{8} = 3.375 \approx 3$$

$$PHB = round\left(\frac{SPV}{NGL} \times H\right) = \frac{2}{8} \times 7 = \frac{14}{8} = 1.75 \approx 2$$

2- Deciding the protected pixels and ignore the LSB of each pixel from the next calculations

In this step of the proposed system, the protected pixels will be determined by taking the rest values of the last row and decided pixel after pixel as illustrated for matrix A in Fig. 9.



a-matrix A b-protected pixels c-New protected pixels values

Figure 9. Deciding and calculating protected pixel

This operation is performed by reading the third pixel in the last row (TPLR) and moving from the first pixel in the image number of pixel equal to the gray level value of (TPLR) as illustrated in Fig. 8 then considering the last position as a starting point and moving from its number of pixels equal to the fourth pixel in the last row and so on until reaching the last pixel in the last row if we need it or reaching last required pixel as illustrated in the following steps. Then in the other calculation ,new values of the protected pixels will be used by ignoring the value of the last bit of the protected pixels in the next calculations as illustrated in Fig. 9.

3- Calculating SVD for each part:

This operation as illustrated in Fig. 6 translate matrix $(A)_{w\times h}$ into three matrices $(U)_{w\times r}$, $(D)_{r\times r}$ and $(V^T)_{r\times h}$ as illustrated in the previous example for matrix (A) by applying SVD on the first part

$$SVD\begin{pmatrix}2 & 1 & 2\\ 4 & 7 & 6\end{pmatrix} \gg U=\begin{pmatrix}-0.2623 & -0.9650\\ -0.9650 & 0.2623\end{pmatrix}, D = \begin{pmatrix}10.4086 & 0 & 0\\ 0 & 1.2890 & 0\end{pmatrix}$$

$$, V^T=\begin{pmatrix}-0.4212 & -0.6834 & -0.5963\\ -0.6742 & 0.6757 & -0.2981\\ -0.6067 & -0.2764 & 0.7454\end{pmatrix}$$

Then the Diagonal of the second matrix (D) will be used in the following calculation by considering it as a horizontal vector as follow*:*

$$HV = (10.4086 \quad 1.2890)$$

4- Calculating norm for each SVD matrices :

In this step of the proposed system, the previous (HV) will be considered for the next calculations for each part of the input image as follows

$$HV = (10.4086 \quad 1.2890)$$

$$norm(HV) = W1 = 10.4881$$

Until this step, we calculated a unique number for a matrix of (2×3) numbers as can be seen if a person changes one number of the six this unique number will be changed as follow

$$SVD\begin{pmatrix}2 & 1 & 2\\ 4 & 7 & 7\end{pmatrix} \gg norm\,(HV) = w_1 = 11.0906$$

And anyone can easily discover that this number (11.0906) differs from the previous one(10.4881).

5- Merging the unique numbers for all parts:

The pre-calculated (*norm*) values for every one of the decided four parts will be merged in this step by suggesting a suitable equation for this purpose as follows

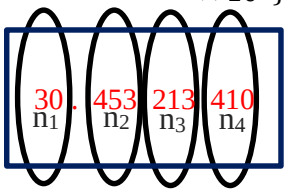
$$w = 2^1 \times w_1 + 2^2 \times w_2 + 2^3 \times w_3 + 2^4 \times w_4 \quad \ldots 3$$

This equation assets various weight for each part but enlarges the value of difference if any pixel will be changed, so for matrix A the following results will be calculated

$$HV_1 = (10.4086 \quad 1.2890)$$
$$HV_2 = (13.5613 \quad 4.4824)$$
$$HV_3 = (16.2159 \quad 5.7924 \quad 0.7026)$$
$$HV_4 = (19.4578 \quad 5.4307 \quad 3.7237 \quad 1.7617 \quad 0.9661)$$
$$w_1 = 11.0906$$
$$w_2 = 14.2829$$
$$w_3 = 17.2337$$
$$w_4 = 20.6398$$
$$w_{Final} = 2 \times 11.0906 + 4 \times 14.2829 + 8 \times 17.2337 + 16 \times 20.6398 = 547.4192$$

The w_{Final}translate into four numbers

$$n_1 = (547) mod\ 1024 = 547$$
$$n_2 = integer\{(w_{Final} - n_1) * 10^3\} = 419$$
$$n_3 = integer\{[(w_{Final} - n_1) * 10^3 - n_2] \times 10^3\} = 200$$
$$n_4 = integer\{\{[((w_{Final} - n_1) * 10^3) - n_2] \times 10^3\} - n_3\} \times 10^3 = 0$$



These equations can be explained a follow

If $w_{Final} = 30.45321341$ then

6- Repeating previous operations four times :

This operation will be performed to take large numbers of possible probabilities to ensure the goal of non –repetitive watermark value, and if the operations take only one number with its four values and each value of them between (0 to 1023) for

integer number and between(0-999) for the floating part so there are only (1024 ×1000×1000×1000) different watermarks and this number is not enough to recognize different pictures. All the previous operation will be repeated by

a- Taking the first row as a guide for watermark discovery operations and start from the last pixel in the image as illustrated in Fig. 10

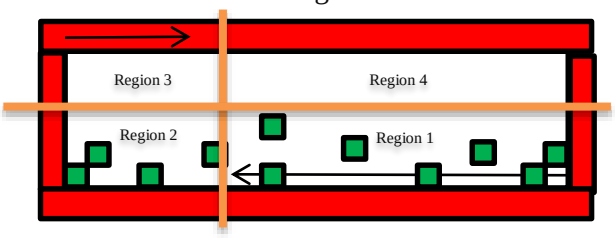


Figure 10. State 2 for calculating watermark numbers

b- Taking the first column as a guide for watermark discovery operations and starting the last pixel in the image as illustrated in Fig. 11.

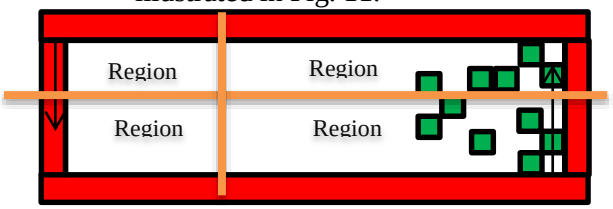


Figure 11. State 3 for calculating watermark numbers

c- Taking the last column as a guide for watermark discovery operations and starting the first pixel in the image as illustrated in Fig. 12.

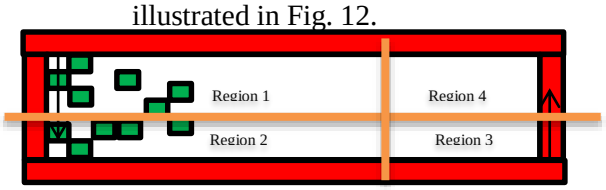


Figure 12. State 4 for calculating watermark numbers

At the end of this step, 8 different numbers represent the value of the watermark of the tested image that must be stored in the image with the suitable operation.

7- *Hiding the final numbers (image watermark) :*

In this step of the proposed system, the sixteen discovered numbers will be hidden in the protected pixels by changing one LSB at most until the finished watermark numbers. In this operation there are sixteen numbers with values between (0 to 1023), this means each number of them needs ten bits to hide within image pixels so, all numbers required (160) bits and the operation for hiding in one bit can be performed as follows

If pixel value(p_v) mod 2 =0 and the bit for hiding is 1 then new p_v =old p_v +1

If p_v mod 2 =0 and the bit for hiding is 0 then new p_v =old p_v

If p_v mod 2 =1 and the bit for hiding is 1 then p_v =old p_v

If p_v mod 2 =1 and the bit for hiding is 0 then new p_v =old p_v -1

After this operation, the final watermark numbers are hidden within 160 pixels in the image.

Results

When the proposed system is applied for discovering the watermark number of testing images the following results will be found for images in Fig. 13, 14, and 15.

Test1:

Figure 13. Image for a test 1.

$for\ first\ state \quad n_1 = 703 \quad n_2 = 33 \quad n_3 = 710 \quad n_4 = 647$

$for\ second\ state \quad n_1 = 960 \quad n_2 = 243 \quad n_3 = 553 \quad n_4 = 56$

$for\ third\ state \quad n_1 = 964 \quad n_2 = 164 \quad n_3 = 273 \quad n_4 = 624$

$for\ fourth\ state \quad n_1 = 799 \quad n_2 = 687 \quad n_3 = 318 \quad n_4 = 67$

$$\mathrm{SNR_{peak}} = 10\log_{10}\frac{(L-1)2}{\frac{1}{N^2}\sum_{r=0}^{n-1}\sum_{c=0}^{n-1}[g(r,c)-I(r,c)]^2} \quad \ldots 4$$

SNR_{peak}=82.65

Test2:

Figure 14. image for test 2.

$for\ first\ state \quad n_1 = 900 \quad n_2 = 352 \quad n_3 = 452 \quad n_4 = 968$
$for\ second\ state \quad n_1 = 405 \quad n_2 = 831 \quad n_3 = 498 \quad n_4 = 730$
$for\ third\ state \quad n_1 = 477 \quad n_2 = 598 \quad n_3 = 226 \quad n_4 = 275$
$for\ fourth\ state \quad n_1 = 749 \quad n_2 = 847 \quad n_3 = 743 \quad n_4 = 152$
SNR $_{peak}$=85.35

Test3:

Figure 15. image for test 3.

$for\ first\ state \quad n_1 = 837 \quad n_2 = 735 \quad n_3 = 537 \quad n_4 = 929$
$for\ second\ state \quad n_1 = 49 \quad n_2 = 292 \quad n_3 = 915 \quad n_4 = 697$
$for\ third\ state \quad n_1 = 259 \quad n_2 = 565 \quad n_3 = 886 \quad n_4 = 903$
$for\ fourth\ state \quad n_1 = 538 \quad n_2 = 898 \quad n_3 = 262 \quad n_4 = 924$
SNR $_{peak}$=90.4

Test4:

Figure 16. image contain text

Original watermark is
for first state $n_1 = 901 \quad n_2 = 235 \quad n_3 = 45 \quad n_4 = 403$
for second state $n_1 = 207 \quad n_2 = 536 \quad n_3 = 210 \quad n_4 = 417$
for third state $n_1 = 207 \quad n_2 = 536 \quad n_3 = 210 \quad n_4 = 412$
for fourth state $n_1 = 413 \quad n_2 = 71 \quad n_3 = 140 \quad n_4 = 723$
SNR $_{peak}$=89.22

Table 1. Watermark values in selected image contain text

Changed position by one degree	n_1	n_2	n_3	n_4
(10,10)	901	241	545	176
	207	536	210	417
	207	536	210	412
	413	71	140	723
(10,250)	901	241	545	176
	207	542	180	26
	207	536	210	412
	413	71	140	723
(290,31)	901	241	545	176
	207	542	180	26
	207	542	180	25
	413	71	140	723
(290,290)	901	241	545	176
	207	536	210	417
	207	536	210	412
	413	114	92	870

Conclusion:

The usage of sixteen numbers in the range of (0 - 2^{10}) make the space of watermark numbers very huge ($2^{10}\times2^{10}\times2^{10}\times2^{10}\times2^{10}\times\ldots\ldots\ldots2^{10}=2^{160}$) with a very low probability of repeating numbers between two different images, so if any very small change occurs in one pixel with less or add only one degree will be effective with noticeable effect on the watermark numbers.

The proposed watermark exploit the stability from the SVD transform with noticeable effect in any simple change in any position of the image as well as the SVD transform make the extracted watermark strong one with no way to change it in simple process or changes.

The famous metric peak signal to noise ratio has perfect value for all cases and the worst case occurs when all protected pixels will be changed in the hiding process (as shown in Table1), this means a change in 160 bits by one degree so the error depends on the size of the image and is very petty in total.

If anyone changes any pixel of the protected regions this makes discovered watermark differ from hidden information and this means discovering change.

Authors' declaration:

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are mine ours. Besides, the Figures and images, which are not mine ours, have been given the permission for re-publication attached with the manuscript.

- Ethical Clearance: The project was approved by the local ethical committee in University of Kufa.

Authors' contributions statement:

A. A. M. contributed to the design and implementation of the research to the analysis of the results and to the writing of the manuscript. N. E. K. contributed to the revision and proofreading of the research.

References:

1. Abdulkreem Mohammed Salih, Abdulkreem Mohammed Salih, Karam M.Z. Othman, Shayma Wail Nourildean. Improved Watermark Criteria Through Mark image. NTU J Eng Technol. 2022; 1(2): 36-39.
2. Jing Liang, Li Niu, Fengjun Guo, Teng Long, Liqing Zhang. VisibleWatermark Removal via Self-calibrated Localization and Background Refinement. Shanghai Jiao Tong University. Arixiv-2108. 03581v1. 8 Aug 2021.
3. Shivanand Pujar, Kangana W.M, Chitrashree Kurthkoti, Abhinandan P. Mangaokar, Jagadish S. Jakati. Advanced Watermarking of Digital Images Showing Robust, Semi-Fragile and Fragile Behaviour. Int J Recent Technol Eng. November, 2021; 10(4): 196-212
4. Dayanand G. Savakar, Shivanand Pujar. Digital Image Watermarking at Different Levels of DWT using RGB Channels. Int J Recent Technol Eng. ISSN: 2277-3878, Jan 15, 2020; 8(5): 559-570
5. Anna Egorova1, Victor Fedoseev. Steganalysis of Semi-fragile Watermarking Systems Resistant to JPEG Compression. Russian Academy of Sciences. Proc 15th IEEE Int Conf Comput Vis, Imaging and Computer Graphics Theory and Applications, Samara, Russia. 2020: 821-828.

https://www.scitepress.org/Papers/2020/91297/91297.pdf

6. Yanxia Jin, Rong Zhu, Xin Qi, Jinrui Zhang, Qifu Cheng, Bo Ma, et.al., An Image Watermark Insertion and Extraction Method Based on EDA-PSO. 2nd International Conference on SEEIE, 2019; chimna: 251-256. https://dx.doi.org/10.2991/seeie-19.2019.58
7. Tarun Agrawal. A Survey On Information Hiding Technique Digital Watermarking. G.L.A. University Mathura, UP, Int J Electr Electron Eng Telecommun.ISSN: 2320-2084, 2015; 3(8): 68-74.
8. Almula B. Sahin, İnan Güler. A Survey of Digital Image Watermarking Techniques Based on Discrete Cosine Transform. Int J Inf Secur Sci. 2021; 10(3): 99-110
9. Tsai S E, Yang S M. A Fast DCT Algorithm for Watermarking in Digital Signal Processor. Mathematical Problems in Engineering. 2017; 2017: 1-7.
10. Khatkale PB, Lokhande DG, Srescoe. Digital Watermarking Algorithm for Color Images. IOSR J Eng. ISSN: 2250-3021, Mar 2013; 3(3): 01-09.
11. Mohammed Ga'fer Alwan, Enas Muzaffer Al-Ta'ee. An Embedded Data Using Slantlet TransformIman. Baghdad Sci J. ISSN: 2078-8665, 2011; 8(3):840-848.
12. Gaurav Chawla, Ravi Saini, Rajkumar Yadav, Kamaldeep. Classification of Watermarking Based upon Various Parameters. Int J Comput Appl Inf Technol. ISSN: 2278-7720, September 2012; 1(2): 16-19.
13. Zhang H, Wang C, Zhou X. Fragile watermarking for image authentication using the characteristic of SVD. Algorithms. 2017 Mar;10(1):27.
14. Hanaa Mohsin Ahmed. Mobile-based Telemedicine Application using SVD and F-XoR Watermarking for Medical Images. Baghdad Sci J. ISSN: 2078-8665, 2020; 17(1):178-189.
15. Jugal K. Verma. Singular Value Decomposition of Real Matrices. Indian Institute of Technology Bombay Vivekananda Centenary College, 13 March 2020. https://math.mit.edu/~gs/linearalgebra/SVD_Slides.pdf.
16. Yan-Bin Jia. Singular Value Decomposition. (Com S 477/577 Notes). 2020: 1-12. https://faculty.sites.iastate.edu/jia/files/inline-files/svd.pdf.
17. Bakthula R, Shivani S, Agarwal S. Self authenticating medical X-ray images for telemedicine applications. Multimed Tools Appl. 2018 Apr 1;77(7): 8375-92.

Open Access **Baghdad Science Journal** **P-ISSN: 2078-8665**
Published Online First: February, 2023 **2023, 20(5): 1797-1807** **E-ISSN: 2411-7986**

العلامة المائية بالاعتماد على تقسيم القيمة المفردة (SVD)

علي عبد العزيز محمد باقر القزاز [1] **نعمه عناد كاظم عبدالله [2]**

[1] كلية التربية، جامعة الكوفة، النجف، العراق
[2] قسم علوم الحاسوب ،كلية العلوم للبنات، جامعة بغداد، بغداد، العراق.

الخلاصة:
العلامة المائية ممكن ان تعرف على انها عملية تضمين معلومات خاصة مطلوبة وقابلة للعكس والتي تجري على ملفات مهمة مطلوب حمايتها لحماية حقوق الملكية للمستند او المعلومات الموجودة في ملف الغطاء وبالاعتماد على علامة مائية من نوع تجزئة او تقسيم القيمة المفردة (SVD). الطريقة المقترحة للعلامة المائية الرقمية تمتلك مدى ضخم جدا من الارقام لتشكيل الرقم النهائي وهذا يعني حماية العلامة المائية من مشكلة التعارض او التداخل . ملف الغطاء يمثل الصورة المهمة التي يراد حمايتها والعلامة المخفية تمثل رقم مميز وحيدوالذي يتم استخراجة من ملف الغطاء بعد اجراء سلسلة من العمليات المتعلقة مع بعضها والمتعاقبة والبدء بتقسيم الصورة الاساسية الى اربعة اجزاء وباحجام غير متساوية. كل جزء من هذه الاجزاء الاربعة يعامل كمصفوفة منفصلة يتم تطبيق تحويل تجزئة او تقسيم القيمة المفردة (SVD) عليها, المصفوفة القطرية يتم اختيارها لايجاد رقم معياري منها. هذه الارقام المعيارية الاربعة يتم معالجتها بطريقه محددة لايجاد رقم مميز وحيد واحد يستخدم كعلامة مائية. وهذا الرقم ممكن تطويره مستقبلا باستثمار صفات اخرى تستخدم في عملية تشكيل الرقم الذي يمثل العلامة المائية عوضا عن عملية تحويل تجزئة او تقسيم القيمة المفردة (SVD) لتشكيل رقمين للعلامة المائية كمل واحد منهم يستخرج بطريقة خاصة وذلك لتجنب بعض التحديات والتغييرات التي تحدث اثناء عملية النقل.

الكلمات المفتاحية: الغطاء، رقم معياري، حقوق الملكية، تجزئة او تقسيم القيمة المفردة، العلامة المائية.