GENETIC ALGORITHM BASED IMAGE WATERMARKING USING SINGULAR VALUE DECOMPOSITION AND INTEGER WAVELET TRANSFORM

G Ramesh babu

Professor, Raghu Engineering College, Tokala V P Sri Chandana

Dept of ECE, Raghu Engineering College, Surupalli Vinuthna Srija

Dept of ECE, Raghu Engineering College, Tummaganti Jitishkumar

Dept of ECE, Raghu Engineering College, Vivek Podagatla

Dept of ECE, Raghu Engineering College

Abstract-

Based on “Redundant Wavelet Transform”, “Singular Value Decomposition”, and “Genetic Algorithm”, this study provides a secure, resilient, and smart watermarking strategy. Here's when the toughness comes in. RWT and SVD are used for feature extraction, while the GA is used for optimization in the proposed watermarking system. In addition, this method presents a signature embedding methodology that would make the watermarked image highly secure. The major technique of protecting intellectual rights and combating piracy is to employ digital watermarking techniques to accomplish electronic copyright. Digital watermarking has stimulated the interest of a huge number of scholars in current history, and it has emerged as a contemporary research priority. In order to get information, this research paper is considered secondary data collection method to gather major information related to the topic.

Keywords: Integer Wavelet Transform, Genetic Algorithm, Singular value decomposition, image watermarking

I. INTRODUCTION

With the fast advancement of information technology as well as the massive dissemination of network connections, businesses and academics have been more worried about the issue of digitized trademarks and the protection of property rights. Digital steganography is an informational security protocol that is associated with hiding the appearance of hidden information during routine communication sessions by encrypting data in another harmless data ensuring that only the originator and intended receiver are informed of the secret's nature [1]. Steganography's popularity has evolved through the years from conventional and ancient techniques to keeping hidden information and media items, particularly secret picture files. Digital watermarking is a powerful tool for securing data, ensuring anti-counterfeiting transparency, and ensuring patent protection. The “Integer Wavelet Transform” (IWT) and the “Genetic Algorithm” (GA) are used in this research to present a new picture watermarking approach. The IWT lowers data redundancy in the derived watermark when compared to traditional wavelet treatments. Since the IWT is shifting consistent, the watermark extraction phase results in a more sophisticated and accurate watermark. The GA is also used to optimize the watermarking parameter, alpha [2]. To secure the watermark's confidentiality, a new signature is inserted in the watermarked picture, preventing the attacker from obtaining the information even if the watermarked image is attacked. This is the major benefit of the suggested strategy, which was lacking in previous approaches.

II. LITERATURE REVIEW

In the subject of data concealment techniques, it is also a significant area and experimental field. The problem of reconciling the algorithm's integrating capability, transparency, and resilience has been a popular and challenging issue in this paper. Watermarking algorithms are split into the spatial domain as well as transform-domain algorithms based on the area of embedding the watermark. The present digital watermarking method's main challenge is to improve the watermark's resilience without compromising its perceptual quality. It also answers how to incorporate multi-signature, steganography, or label copyright holders simultaneously [3]. Singular value decomposition (SVD) has been shown to effectively recover the transmitted signals, with the power of the retrieved singular value diminishing with time and the ability to recover the maximum benefit of watermark energy. Furthermore, the single value is stable. As a result, the singular value watermark mechanism can meet the goal of watermark resilience. Object recognition in video analysis systems is steadily improving in terms of quality, thanks to a wide range of applications that include critical

procedures such as the analysis of unusual evens [4]. Not only that, but it could also be used to characterise human proportions, count people in crowds, identify specific traits, classify people based on gender, predict falls in the elderly, and so on.

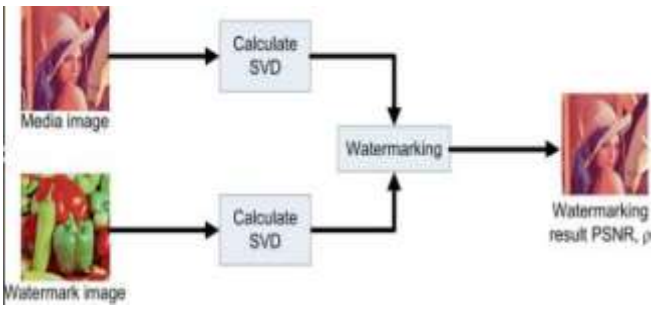

Fig 1: Block diagram of image watermarking using SVD method

(Source: [4])

As a result, the current common watermarking approach generally uses this method to increase the watermark's resilience. To overcome the ownership difficulty, many picture steganographic methods that are based on singular value decomposition have been developed. The original host picture, as well as the watermark image, create a complete structure of the image watermarking procedure. Using a watermark embedding method, the watermark image is placed into the host picture, resulting in a watermarked picture that is conveyed via the network system and vulnerable to different assaults [5]. The technology then uses the watermark extraction technique to retrieve the watermark information from the watermarked picture. Imperceptibility, reliability, potential, as well as confidentiality, are the four design concepts of a digital image watermarking framework. These needs, however, cannot be met concurrently due to their restricted and competing qualities. In most cases, the balance between imperceptibility, reliability, and potential is determined by the application. Furthermore, research has shown that spatial domain approaches are less resilient than transform domain approaches. The data is integrated in the transform domain approach by changing an image's coefficient with techniques including "***discrete cosine transform***" (DCT), "***Set partitioning in hierarchical trees"*** (SPIHT), "***Curvelet transform***" (CLT), ***discrete wavelet transform*** (DWT), along with "***singular value decomposition"*** (SVD) [6].

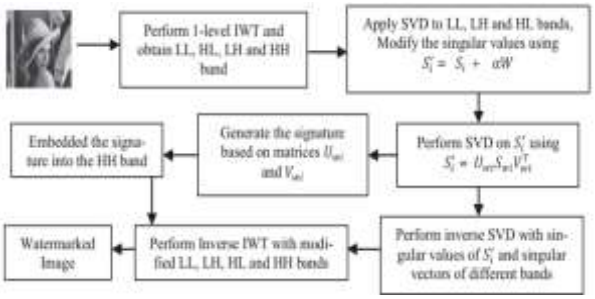

Fig 2: Extract watermarking using SVD method

(Source: [6])

Based on the region of embedding the watermark, steganography techniques may be divided into two groups. The first category includes methods that employ the spatial domain to hide data, whereas the second group uses transformation regions such as discrete cosine transform (DCT), discrete Fourier transform (DFT), and discrete wavelet transform (DWT) for steganographic. Despite the fact that spatial domain techniques are simpler and less sophisticated, all spatial domain picture watermarking systems have the same drawback: lower trustworthiness. The attacker can more readily obtain the underlying data due to the image depiction in its initial form [6]. Furthermore, past research shows that, when compared to spatial transformation techniques, transform domain techniques are often more resilient to noise, standard image analysis, and compression.

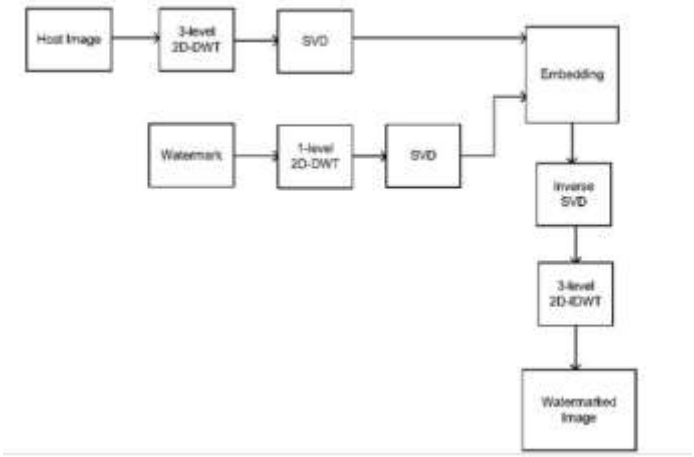

Fig 3. Block diagram for watermark embedding process

(Source: [7])

A secure picture watermarking system that relies on the integer wavelet transform and singular value decomposition has been suggested. However, due to the IWT, the latency in this strategy appears to be greater. Due to its advantages, singular value decomposition (SVD) has become widely employed in the field of picture watermarking in current history. Furthermore, several experts have pointed out that most SVD-based approaches have a false positive detection algorithm. Several academics have developed upgraded versions of SVD-based picture watermarking systems to address this issue [7]. Based on how SVD is implemented, there are two variations of this arrangement: full cover picture and block-wise. By introducing a compensating procedure, the imperceptibility of a picture watermarking methodology based on lossless compression SVD introduced is strengthened. Despite the fact that the features extracted are resistant to a wide range of assaults, the efficacy of the watermarking technique is also dependent on the watermarking constant.

III. METHODOLOGY

Integration of secondary data collection method helps to get realistic and appropriate information from different journals and articles. This research paper includes the generic algorithm-based image watermarking by using advanced technology or methods such as SVD and IWT. Throughout this research, researchers have collected know the based concept of SVD for image watermarking. For data collection, secondary qualitative method is considered to gather relevant and theory-based information according to the topic. Research questions are listed below.

- What are the methods mainly used for image watermarking?
- What are the risk factors related to singular value decomposition for modifying watermarking in images?

IV. ANALYSIS AND INTERPRETATION

There have been several techniques to improve the watermarking constant that has been presented previously. PSO is a smart algorithm that effectively addresses using a stochastic, population-based computer programme. Digital filtering algorithms are used to generate a period approximation of a digital signal in DWT. At various scales, the information to be studied is routed via filtration with various frequency ranges. Every DWT level of segmentation divides a picture into four sub-carriers: LL, HL, LH, and HH. Filtering the digital signal through a low-low filter (LL) in both ways yields the different resolutions estimation sub band, which provides an approximate representation of the image. The HL and LH sub bands are created by sending the signal through a low-pass filtration system in one way and a high-pass filter in the other. The high-frequency elements along the diagonals are included in the HH sub band, which is high-pass screened in both directions. The “invisible watermark” is a sophisticated concept that is used to recognise and create copyright data. The principle of a transparent watermark is akin to impressing a mark on paper typically used in paper material to identify owner or source.

Fig 4. Test cover images

(Source: [6])

Depending on the area of the embedding process, "***digital watermarking methods***" can be divided into two groups. Despite the fact that "spatial domain techniques" are simpler and less sophisticated, all "spatial domain picture watermarking techniques" have the same drawback: lower security.

- ***Proposed SAGRU Approach***

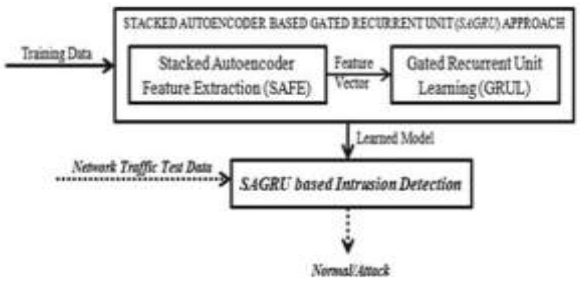

Fig 5. Block schematic approach of proposed SAGRU Approach

(Source: [7])

"Stacked Autoencoder Feature Extraction" (SAFE), "***SAGRU-based intrusion detection"*** along with "***Gated Recurrent Unit Learning"*** (GRUL) are the three components that make up the SAGRU technique. The SAFE module identifies the relationship between features and extracts the elements from the training examples dynamically. GRUL uses feature extraction to avoid the "vanishing gradient" problem by retaining necessary details and dismissing unnecessary facts. In data sets, the learned SAGRU model is utilised to detect incursions. In the above figure it shows a block diagram of the proposed "***SAGRU intrusion detection technique***".

- ***Singular value decomposition (SVD)***

Singular value decomposition or SVD is a useful method in linear algebra that's used in a variety of study domains, including statistical method, "data compression" as well as "canonical correlation analysis". Let X denote an "MN-dimensional matrix". Eq. can be used to describe the decomposition for X. (1),

$$X = \begin{bmatrix} X(1,1) & X(1,2) & \cdots & X(1,N) \\ X(2,1) & X(2,2) & \cdots & X(2,N) \\ \vdots & \vdots & \ddots & \vdots \\ X(M,1) & X(M,2) & \cdots & X(M,N) \end{bmatrix}$$

$$X = USV^T \qquad (1)$$

The elements U and V are made up of eigenvectors from matrix X, while T stands for conjugate transposition. The left eigenvector and right eigenvector, correspondingly, are the U and VT elements. The two aspects are also orthogonal matrices, as indicated by Eq (2),

$$I_M = U_M^T U_M$$
$$I_N = V_N^T V_N$$

The identity matrices IM and IN have sizes of MM and NN, respectively. The element S is a square matrix of non-negative real values, and it is a singular value matrix in the SVD area.

$$S_{MN} = \begin{bmatrix} \sigma(1,1) & 0 & \cdots & 0 \\ 0 & \ddots & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma(M,N) \end{bmatrix} \quad (3)$$

Where $\sigma(1,1) \geq \sigma(2,2) \geq \cdots \geq \sigma(M,N) \geq 0$

- ***Genetic algorithm***

In the field of developmental computation, an evolutionary algorithm is one of the most extensively used artificial intelligence algorithms. A simple GA is generally made up of three steps: selection, genetic operation, and substitution. Initially, a species is formed at random. The optimization algorithm then evaluates each chromosome's fitness using objective values from the optimal solution. In other words, by assembling chromosomes, the genetic algorithm imitates people in the community of organisms, and by choosing and cross-mutating genetic material, it imitates the reproducing and development of all things in the community of organisms. The better-fitting chromosome has a better chance of surviving during evolution. The optimal solution is problem-specific, and its strategy for achieving this can be interpreted as a system performance measure. Then, from the community, a certain set of chromosomes is chosen to be parents. After that, genetic operations such as crossover operator are used to create children from these sources.

VI. CONCLUSION

This paper provides an image watermarking system that is resilient, consistent, and imperceptible, and is predicated on a combination of "3 Level DWT" along with "SVD with the MWOA". A new picture watermarking method based on redundancy "***wavelet transform and Genetic Algorithm***" has been developed. GA is used to optimise the strength of copyrighting constructs such that a trade-off between resilience and interpretability can be made. Simulation is carried out on a variety of visuals as well as attacks. The GA algorithm is used to select an optimum alpha value by taking into account all of the attacks. This method concentrated on the entire sub bands acquired after RWT for embedding. This method, however, achieves a high level of resistance to all forms of attacks.

REFERENCES

[1] Zhu, T., Qu, W. and Cao, W., 2022. An optimized image watermarking algorithm based on SVD and IWT. The Journal of Supercomputing, 78(1), pp.222-237.

[2] Mood, N.N. and Konkula, V.S., 2018. A novel image watermarking scheme based on wavelet transform and genetic algorithm. International Journal of Intelligent Engineering and Systems, 11(3), pp.251-260.

[3] Begum, M., Ferdush, J. and Uddin, M.S., 2021. A Hybrid robust watermarking system based on discrete cosine transform, discrete wavelet transform, and singular value decomposition. Journal of King Saud University-Computer and Information Sciences.

[4] Thanki, R., 2020. Genetic algorithm-based intelligent watermarking for security of medical images in telemedicine applications. In *Intelligent Data Security Solutions for e-Health Applications* (pp. 185-204). Academic Press.

[5] Maloo, S., Kumar, M. and Lakshmi, N., 2020. A modified whale optimization algorithm based digital image watermarking approach. *Sensing and Imaging*, *21*(1), pp.1-22.

[6] Song, L., Sun, X.C. and Lu, Z.M., 2020. Robust blind watermarking algorithm based on contourlet transform with singular value decomposition. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*.

[7] Devi, H.S. and Singh, K.M., 2020. Red-cyan anaglyph image watermarking using DWT, Hadamard transform and singular value decomposition for copyright protection. *Journal of Information Security and Applications*, *50*, p.102424.