International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

SVD Based Authentication in Remote Health Monitoring System

Haritha M.[1], Bijin Bodheswaran[2]

[1]M .Tech Student, Department of Communication Engineering, Sree Buddha College of Engineering for Women, Elavumthitta, Kerala, India

[2]Assistant Professor, Department of Electronics and Communication Engineering, Sree Buddha College of Engineering for Women, Elavumthitta, Kerala, India

Abstract: ***Remote health monitoring system is a technology to enable monitoring of patients outside the hospitals (e.g. in the home), which may help to increase access to care and reduce the cost of healthcare. Patient's authentication is a necessary security requirement in remote health monitoring system in order to verify whether the sensors are monitoring the right person or not. In this paper, we present a SVD based authentication in remote health monitoring system in order to determine the claimed identity is true or false. The proposed method employs a cascade of two transforms; the 4 level-discrete wavelet transform and the singular value decomposition (SVD). The major steps includes; the watermark embedding procedure, watermark extraction procedure and the verification procedure. The data to be authenticated is encrypted using SHA-1 algorithm used as the watermark bits which is embedding on the singular values of the DWT sub-bands of the sensor data. The claimed patient is verified by comparing the extracted watermark bits with the hash database at the authentication server.***

Keywords: Authentication, Watermarking, Hash, Singular value decomposition, 4-level discrete wavelets transform.

1. Introduction

Traditional healthcare systems struggle to cope up with increasing demand and rising costs. Mobile computing and medical sensor technology offer a new paradigm for healthcare, namely remote healthcare monitoring system [1], that can reduce the cost and improve the quality of healthcare services. Mobile medical sensors promise to provide an efficient, accurate, and economic way to monitor patient's health outside the hospital. Patient authentication [2] is a necessary security requirement in remote health monitoring system in order to verify the sensors are monitoring the right person. If someone else wears the patient's sensors, with or without the patient's permission, it could be made incorrect medical decision. Hence, the monitoring system needs to make sure that the data is coming from the right person before any medical or financial decisions are made based on the data.

Digital watermarking technology is a new attractive method of protecting against unauthorized copying of digital multimedia files that includes image, audio and video components. Digital watermarking [3] aims at embedding a watermark in the original file without introducing perceptual degradation. The embedded watermarks may be generated to refer to originators, receivers, unique serial numbers, or time stamps. On the basis of human perception, the watermarking can be divided into visible and non visible watermarking. In the case of invisible watermarking, the output signal does not change much when compared to the original signal. Hence it's more robust to signal processing attacks when compared to visible watermarking. As the quality of the original image does not suffer much, it can be used in almost all the applications. Frequency-domain watermarking techniques usually use DFT (Discrete Fourier Transform), DCT (Discrete Cosine Transform), or DWT (Discrete Wavelets Transform) to transform the signal to locate appropriate embedding location [4]. The singular value decomposition (SVD) of a matrix is one of the fundamental tools of numerical linear algebra. It can be performed on any real (m, n) matrix. It has applications to regression analysis, data compression and numerical linear algebra among others [5].

In this paper, we introduce a SVD based authentication in remote health monitoring system in order to avoid the unauthorized access. The algorithm used the attractive properties of two powerful mathematical transforms; the Discrete Wavelet Transform (DWT), and the Singular Value Decomposition (SVD). In the proposed algorithm, hashed patient's names (watermark bits) are embedded on the elements of singular values of the DWT sub-bands of the original frames and to produce the watermarked signal.

2. Transform Basics

2.1 Discrete Wavelets Transform

Discrete Wavelet transform (DWT) is a mathematical tool for hierarchically decomposing an image. It is useful for processing of non-stationary signals. The transform is based on small waves, called wavelets, of varying frequency and limited duration. Wavelet transform provides both frequency and spatial description of an image [9]. DWT produces two sets of coefficients namely, the approximated coefficients (A) (low frequencies) and the details coefficients (D) (high frequencies). Depending on the application and the length of the signal, the low frequencies part might be further decomposed into two parts of high and low frequencies. The original signal *S* can be reconstructed using the inverse DWT process. For a 4-level DWT decomposition of signal *S* can be written as;

$$\begin{aligned} S &= A_1 + D_1 \\ &= A_2 + D_2 + D_1 \\ &= A_3 + D_3 + D_2 + D_1 \\ &= A_4 + D_4 + D_3 + D_2 + D_1 \end{aligned} \quad (1)$$

The DWT is very suitable to identify areas in a signal where a watermark can be embedded effectively.

2.2 Singular Value Decomposition

Singular value decomposition is said to be a significant topic in linear algebra by many renowned mathematicians. Special feature of SVD is that it can be performed on any real (m, n) matrix [10]. It has applications to regression analysis, data compression and numerical linear algebra among others. A singular value decomposition of an n × n real-valued matrix A can be factorized as; $A = USV^T$, where U and V are $n \times n$ orthogonal matrices, and S is a diagonal matrix with nonnegative entries.

3. The Proposed Method

The proposed method employs a cascade of two transforms; the four level-discrete wavelet transform and the singular value decomposition. The method is described in this section by outlining the major steps in its three procedures; the watermark embedding procedure, watermark extraction procedure and the verification procedure.

3.1 Watermark Embedding Procedure

The watermark embedding procedure is illustrated in the block diagram shown in Figure 1, and described in details in the steps which follow.

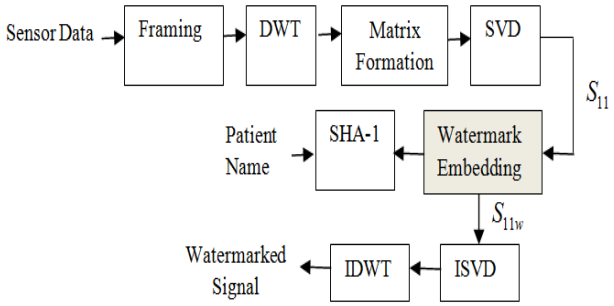

Figure 1: Block diagram of watermark embedding procedure

3.1.1 Algorithm

Step1: Perform a 4 level-DWT on a single frame of the original sensor data.

Step2: This operation produces five coefficients such as A4, D_1, D_2, D_3, D_4 are used to make a matrix (say A). The D's represent the details coefficients and A_4 represents the approximation coefficient.

Step3: Decompose the A matrix using the SVD operator and produces the three orthogonal matrices U, S and V^T as follows:

$$A = USV^T, \quad (2)$$

where S is the diagonal matrix.

$$S = \begin{bmatrix} S_{11} & 0 & 0 & \dots & & \dots & & 0 \\ 0 & S_{22} & \dots & \dots & & 0 & \dots & 0 \\ . & 0 & & & & & & \\ . & . & & & S_{rr} & \dots & & \\ . & . & & & & & & \\ 0 & 0 & \dots & & \dots & & \dots & S_{nn} \end{bmatrix} \quad (3)$$

The diagonal S_{ii} entries are the non-zero singular values of the matrix A [4]. The S_{11} value is subjected to watermark embedding process.

Step4: Embed the hashed patient name (watermark bits) into the DWT-SVD-transformed sensor signal and to produce the watermarked signal according to the following formula:

$$S_{11w} = S_{11} + alpha \times w(n), \quad (4)$$

where $w(n)$ is the watermark bit and the S_{11} is the top left value in the S-matrix, and S_{11w} is the watermarked S_{11}.

Step5: Perform ISVD and IDWT transform on the watermarked signal in order to convert time to spatial domain.

3.2 Watermark Extraction Procedure

The watermark extraction procedure processes the watermarked signal and the singular value of a single frame of the original sensor data. The procedure is illustrated in the block diagram shown in Figure 2, and described in details in the steps which follow.

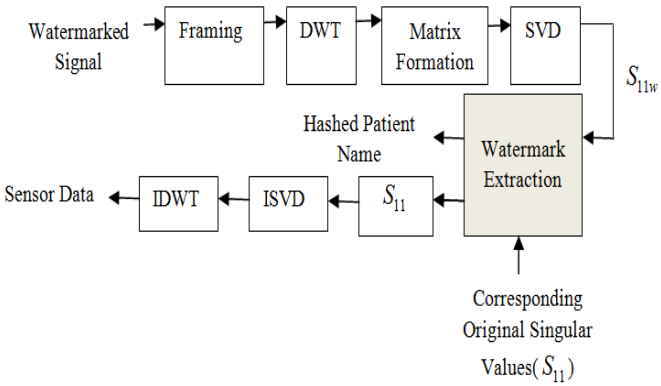

Figure 2: Block diagram of watermark extraction procedure

3.2.1 Algorithm

Step1: Perform steps 1 through 3 of the embedding procedure until the *S* matrix is obtained.
Step2: Extract the same hashed data using the equation given below:

$$w(n) = \frac{(S_{11w}/S_{11} - 1)}{alpha}, \quad (5)$$

where $w(n)$ is the watermark bits, S_{11w} is the watermarked signal and S_{11} is the singular value of the original frame.

3.3 Verification Procedure

In the verification procedure, the system decides whether the claimed identity is true or false. The procedure is illustrated in the block diagram shown in Figure 3, and described in details in the steps which follow.

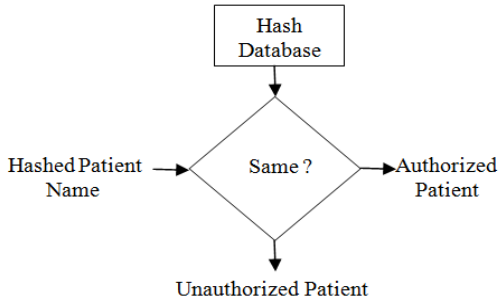

Figure 3: Block diagram of verification procedure

3.3.1 Algorithm

Step1: Compare the extracted watermark (hashed patient name) with the hash database at the authentication server.
Step2: The claimed identity is true if the extracted hash is found on the hash database.
Step3: If the extracted hash is not found on the hash database, then the claimed patient is rejected.

4. Simulation Results

MATLAB R2013a is used as a platform of programming for this project.

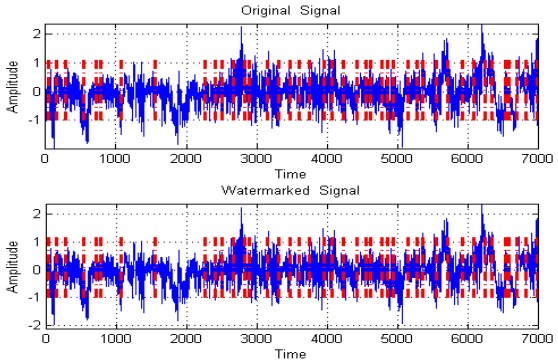

Figure 4: Original and watermarked signals (alpha=0.1)

The original signal (signal from the sensors) and watermarked signal are shown in Figure 4. The watermarked signal is generated by embedding the original signal with the encrypted patient name. The encryption is done by hashing the patient name using SHA-1 algorithm. The patient verification result for a valid patient is shown in Figure 5.

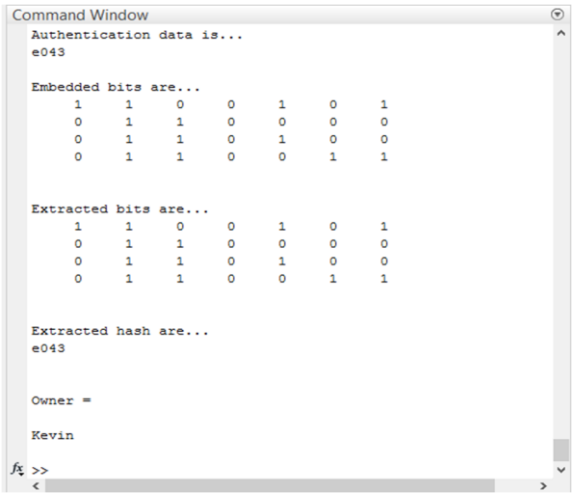

Figure 5: Verification result for a valid patient

In the command window, the data to be authenticated (Kevin) is hashed (e043) at the transmitter side. At the receiver side, extracting the same hash from the watermarked signal and performed the verification procedure at the authentication server. If the extracted hash can be found on the hash database, then the claimed patient is declared as valid one. Otherwise the claimed identity is rejected as shown in Figure 6.

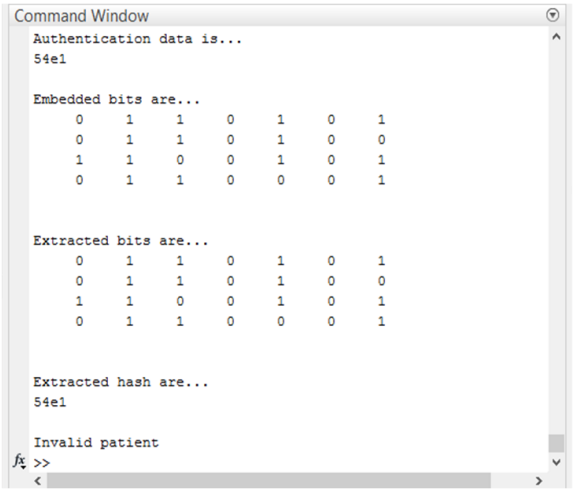

Figure 6: Verification result for an invalid patient

5. Conclusion

A remote health monitoring system relies on the ability of the system to correctly authenticate a patient. Patient authentication verifies whether the sensors are monitoring the right person, so that healthcare professionals can provide appropriate health services.

This paper proposed an authentication technique in remote health monitoring system using SVD. The proposed method employs a cascade of four level-discrete wavelet transform and the singular value decomposition**.** The major steps included; the watermark embedding procedure, watermark

extraction procedure and the verification procedure. The data to be authenticated is encrypted using SHA-1 algorithm used as the watermark bits which is embedding on the singular values of the DWT sub-bands of the sensor data. The claimed patient is verified by comparing the extracted watermark bits with the hash database at the authentication server**.** This is an effective method in order to determine the claimed patient is valid or not in a remote health monitoring system.

6. Acknowledgment

I would like to express profound gratitude to our Head of the Department, Prof. Cherian Schariah, for his encouragement and for providing all facilities for my work. I express my highest regard and sincere thanks to my guide, Asst. Prof. Mr. Bijin Bodheswaran, who provided the necessary guidance and serious advice for my work.

References

[1] N. Oliver and F. Flores-Mangas, "HealthGear: a real-time wearable system for monitoring and analyzing physiological signals," In Proceedings of the International Workshop on Wearable and Implantable Body Sensor Networks (BSN), April 2006.

[2] Janani Sriram,,Tanzeem Choudhury and Minho Shin, "Activity-aware ECG based authentication for remote health monitoring, "ICMI-MLMI'09,Novenmber 2009.

[3] Gaurav Chawla, Ravi Saini and Rajkumar Yadav, "Classification of Watermarking Based upon Various Parameters," IJCAIT. Vol. I, Issue II, September. 2012.

[4] J. S. Dhage, A. K Gulve, "An Efficient Approach on Audio Watermarking: Cascading of the Discrete Wavelets Transforms and Singular Value Decomposition," special Issue of ICEICE,December 2011 .

[5] Clifford Bergman and Jennifer Davidson, "Unitary Embedding for Data Hiding with the SVD," Security, Steganography and Watermarking of Multimedia Contents VII, SPIE Vol. 5681, January 2005.

[6] www.mathworks.in

[7] Andrews, H., & Patterson, C., "Singular Value Decomposition (SVD) Image Coding," IEEE Transactions on Communications; 42(4): 425-432.

[8] Mohammad, A., Al-Haj, A., & Shaltaf, S., "An improved SVD-based watermarking scheme for protecting rightful ownership," Signal Processing Journal; 88(9): 2158- 2180.

[9] Jyoti sahu and Dolley shukla, "Digital Image Watermarking Method 4 Level DWT-DCT on the Basis of PSNR", 2015 IJEDR | Volume 3, Issue 2 | ISSN: 2321-9939.

[10] Lijie Cao, "Singular Value Decomposition Applied To Digital Image Processing," Arizona State University Polytechnic Campus Mesa, Arizona 8521.

Author Profile

Haritha M received the B-Tech degrees in Electronics and Communication Engineering from M.G University, Kerala at Sree Buddha College of Engineering for Women in 2014. And now she is pursuing her M-Tech degree in Communication Engineering under the same university in Sree Buddha college of Engineering for women.

Bijin Bodheswaran working as Assistant Professor in department of Electronics and Communication, Sree Buddha College of Engineering for Women, Elavumthitta, Pathanamthitta.