International Journal of Advanced Science and Technology
Vol.117 (2018), pp.11-28
http://dx.doi.org/10.14257/ijast.2018.117.02

Secure Authentication, Privacy and Integrity in Telemedicine using Visual Cryptography

Arvind Bakshi[1,*] and Anoop Kumar Patel[2]

[1,2]Department of Computer Engineering, National Institute of Technology, Kurukshetra-136119, Haryana, India
[1]arvind_31603127@nitkkr.ac.in, [2]akp@nitkkr.ac.in

Abstract

Today, the whole world is facing the problem of scarcity of good doctors, especially in rural and remote areas. The overall condition of medical facilities is on derogatory. To resolve this issue, telemedicine techniques are under development. It provides cost-effective and quality medical services at remote and rural places. In this medical services are provided at a distant location by a doctor sitting in some big city using information technology where data like medical images (CT scan, MRI etc.) are used for diagnosis. Medical report and prescription by a doctor are also provided from distant places using information technology (IT).

But this confidential and sensitive data are under threat of attack on a public network, so must be secured. One of the solutions for securing this data is visual cryptography (VC) approach that creates some set of shares for an image. These shares are transmitted over the network. The decryption method is fully mechanical and executes in the fixed complexity of $\Theta(1)$. In this article, we have proposed an algorithm that is 2 out of 2 visual cryptography scheme for a grayscale image. It shows the shares of the original image that have no visual information. At the receiver end when the shares are overlapped (in XOR fashion), all information is revealed.

Keywords: *Authentication, Integrity, Privacy, RONI, Security, Telemedicine, Visual Cryptography*

1. Introduction

Today's world is changing very rapidly and people's lifestyle is also changing. People are living high technology based lifestyle, still, a large section of society is facing the issue of quality medical health care. The doctor-patient ratio is quite poor globally [1]. Good, specialized doctors are only available in big cities and thus rural and remote areas are facing a problem of quality medical care. As the world population grows every year, the health centres along with medical staff should also increase proportionally to fulfil the demand but this is not happening [1]. In such cases, telemedicine can be an effective solution to provide good medical care to everyone. Telemedicine is the set of technologies that provide the medical facility from a distance. World health organization defines telemedicine as, “The impartment of medical care, from a distant place, by all health care professionals using information and communication technologies by exchanging valid information for diagnosis, treatment and prevention of disease and injuries, research and evaluation, and for the continuing medical education, all in the regard of leading the well-being of respective and their neighborhood” [1]. Telemedicine can be broken into three main categories: store-and-forward (involves collection of medical data of patient and then sending it to some specialist later), remote patient monitoring (in this patient is

Received (March 11, 2018), Review Result (May 11, 2018), Accepted (May 24, 2018)

[*] Corresponding Author

ISSN: 2005-4238 IJAST

constantly monitored by some specialist at some far off place using electronic devices) and real-time interactive services (in this doctor and patient communicate at a time using information technology) [1].

Telemedicine doesn't replace the traditional medical practice but it supplements it [1]. It can also provide expert doctors to health centres via the use of information technology from some distant place that lacks' specialists. Here every person throughout the globe who has internet facility can access services of good doctors by connecting with telemedicine network. It is also an economical and time-saving solution for getting medical services [1].

There are a number of new diseases reported very often throughout the globe and diagnosis and treatment of these diseases takes some time. It causes severe and ambiguous situation even for a doctor (especially for communicable diseases), how to diagnose and treat. Using telemedicine different specialists of the world can put their concern and find a solution in very less time. Many times, the possibility of spreading of infectious disease, parasites between patients and medical staff, are reported like Ebola, MRSA (Methicillin-resistant Staphylococcus aureus). Additionally, some patients feeling uneasy at hospital or clinic are better treated using telemedicine, for example, people suffering white coat syndrome. Patients who are shut-in or need a special vehicle like an ambulance to move them, for example, people with excess body weight or physically challenged people can also benefit a lot from telemedicine. Telemedicine can also be used for spreading medical skills and geographical experience of a disease. Apart from above, there are many challenges to telemedicine, some of them are as follows: [2]

- **Challenge-1 (Administrative):** The hospital administration always looks for profit but sometimes telemedicine infrastructure becomes so costly that cannot produce desired profits. But in the future when people will be more familiar and comfortable with the telemedicine technology then the application and revenue will increase.

- **Challenge-2 (Physician):** Although physicians make use of electronic gadgets on daily basis, they might not be very much expert to use some professional medical devices for telemedicine and some of them are also not interested to use this technology. There are a number of reasons for it, some of them are as follows [2].

    1. They may lack interest in depending on technology for treatment.
    2. They may lack interest in undergoing any training that may be required to make use of the equipment.
    3. They may lack trust in electronic equipment and may fear its breakdown making a pause in the treatment, for *e.g.*, a dropped connection between a doctor and a patient could lead to missed instructions and possible patient mismanagement and wrong treatment.
    4. Physicians do not go into complexities of legal issues for using telemedicine such as credentialing, reimbursement, malpractice, insurance etc.
    5. Physician may also have a concern about potential security risk that breaks the confidentiality of patient, access to the different functionality of telemedicine device in an unauthorized way and to the stored data.

- **Challenge-3 (Infrastructure):** Telemedicine needs good infrastructure like high-speed internet, imaging technology or peripherals, access to technical support staff, staff training [4].

- **Challenge-4 (Sustainability):** It states that whether a hospital will be able to run telemedicine services once started.

Apart from the above mentioned general challenges, security of telemedicine services is a major challenge. Insecure telemedicine service can cause a problem to the patient in terms of manipulated (by an attacker) data analysis by a doctor that always leads to the wrong prescription. An attacker can also steal some confidential information that may be used for extortion in future. Some of the threats of telemedicine are as follows [3] [4] [5] [6]:

- Authorization/Authentication
- Accountability
- Information security
- Privacy/Confidentiality
- Reliability
- Integrity
- Physical security of data at telemedicine centre
- Network Security Protocols
- Policy and Standards
- Legal issues

Our work applies the approach of Visual Cryptography on images used in telemedicine to provide secure information exchange. Although existing approaches like watermarking, data and image encryption etc. exist but they are complex and vulnerable to attack in which encryption key can be compromised. Existing techniques also take huge time and have a complex process of decryption. In the proposed Visual Cryptography approach we create more than 1 share for image data and send to more than 1 authorized person of same telemedicine centre that is decrypted using a mechanical process of combining shares. It is based on the original Visual Cryptography approach by Naor and Shamir [7]. We have proposed a new algorithm which does not encrypt whole image but only RONI (region of non-interest) of the image that contains signature information (SI) like patient ID *etc.*, a separator, and digest of some portion of the image.

The paper is categorized into 6 major sections. The first section of the article is the introduction that describes fundamentals of telemedicine and its security challenges. In the second section, we have discussed the fundamental concept of telemedicine security and visual cryptography approach that provides security to the telemedicine data. In the third section, we have discussed the proposed algorithm using visual cryptography. It describes the fundamental steps that are followed in order to create shares of the original image. In next section, we have shown and analyzed results of the proposed algorithm. In the fifth section we have concluded our work and in the last section, we have talked about the future scope of the work.

2. Telemedicine Security Challenges and the Concept of Visual Cryptography

2.1. Telemedicine Security

Here we have discussed security challenges in telemedicine such as integrity, authentication and privacy. There are some existing solutions to these challenges as in Table 1. We have also analyzed these in details. We have discussed following three security challenges:

1. **Integrity:** This ensures that the information sent from sender to receiver is not modified during the transmission period. For medical data, integrity means that data is received as it is sent by sender while it is transmitted via electronic medium. There might be a possibility of modification in sender's data due to data compression and transmission errors, thus it becomes necessary to differentiate between malicious and innocent modifications. There should be a mechanism to detect unauthorized modification somewhere between sender and receiver. Coatrieux *et al.*, proposed system that achieves integrity objective in terms of 3 levels [3]:

    - **Level-1 (Modification detection):** Whether the image is modified or not?
    - **Level-2 (Modification location):** Which parts of the image are modified?
    - **Level-3 (Forensics/integrity analysis):** Whether the modification is malicious or innocent?

Hui Huang [3] extended the work of Coatrieux *et al.*, and worked on Level-3 only. He combines blind and non-blind techniques (in blind technique no prior information is available whereas in non-blind technique some amount of information is there). The non-blind technique can only detect the local modification in the image and blind technique integrates local modification to detect all possible modifications in the image. Hi Huang defines 3 mechanisms for integrity [3]:

- *Signature-based method (Digitally signed image):* based on hash comparisons, Cryptographic hash functions are used.
- *Watermark-based method:* either addition or substitution based watermarking can be used.
- *Image forensics method:* There are two methods for this active and passive. In the active method, the watermark is embedded at source while inspected at verification stage. In passive method blind approach is used.

Signature-based method, watermark based method and active image forensics method belong to the category of non-blind techniques as they require prior information of the original image to detect modification. Since original image is not always available thus blind methods are often used [3]. Watermarking techniques have the limitation that they can be better embedded during the image creation time but its visual quality is affected when it is embedded after image creation. Watermarking provides better visual perception in images which have object generation capabilities.

2. **Privacy:** Privacy refers to the denial of access to information by unauthorized individuals. The big challenge for telemedicine is that to maintain the privacy of patient's health information over secure and insecure channels. Patient's information can be misused at any level that's why it is essentially required to maintain its privacy. To provide telemedicine services everywhere it should be secure enough over the public network *e.g.*, library, coffee shop *etc*. To make it secure, the different end to end encryption algorithm and other security technologies are used to prevent information theft and tampering. Patients should be trained enough to take necessary precautions while using public and private networks for telemedicine. Medical identity may also be used for obtaining medical services by proxy patients.

    Hodge *et al.*, have proposed health information privacy laws for a legal emend concerning privacy that includes [8]:

    - Sighting accountable health-related information as highly delicate.
    - Granting privacy shields established on fair practices.

- Granting the patients with the knowledge and rights against consent to disclosure.
- Restricting the leak of healthcare data in case of non-consent.
- Integrate known industry-wide security practices.
- Install a national level health information protection authority.
- Implement a nationwide nominal level of privacy protections.

The privacy breach is especially vulnerable to patients, such as those with AIDS or mental illness, may be denied jobs, credit, insurance, or even their dignity. For example, a New York Congresswoman had her medical records, including information about her depression and a suicide attempt, faxed to the media in the midst of her political campaign [9]. Hackers have a large incentive to misuse patients' private health information because it can be a profitable asset to employers, insurers, and other people [9]. Thus the potential brokerage of this information is quite likely and in some cases lethal. Shifali *et al.*, in mobile health (mHealth), a new growing branch of telemedicine where the mobile sensors are used to constantly monitor patient has also posed some privacy challenges [10]. In mHealth, the sensitivity and quantity of health information collected via mobile devices are an issue for privacy and security. To secure the privacy of data, we use some safeguards such as the type of information being used, the intended usage of the mHealth tool, and the technique of sharing information, the costs of protection all should be balanced to make it more secure. The above system obtained has minimum privacy risk. Keerthana *et al.*, use Steganography to provide privacy protection to medical data for telemedicine applications [11].

The proposed technique ensures secure information hiding with negligible distortion of the host signal. It avoids the unauthorized user from extracting hidden information. The technique is defined using the following 5 steps in which first 4 are used for encryption and the last one is used for decryption [11]:

1. *Choas cryptosystem:* In this stage, each pixel values of the input image is XOR'ed with the key value generated from the chaotic sequence thus giving as output an encrypted pixel image.
2. *Wavelet transform:* This stage comprises of performing a wavelet transform using short time Fourier transform. In wavelet transform, the input signal is projected onto a complete set of translated, dilated versions of the mother wavelet. Also forward (gives H and L values) and reverse (gives inverse integer wavelet transform) lifting in IWT is used.
3. *Adaptive LSB Embedding:* In this, the input message is decomposed into bits, then coefficients from high-frequency bands are selected say cf. The number of bits for payload are chosen. Then, least significant bits of cf is replaced with most significant bits of the decomposed input message.
4. *Inverse wavelet re-composition:* This stage consists of obtaining a new watermarked ECG signal by application of inverse wavelet packet recomposition on the watermarked 32 sub-bands obtained from the previous step. The inverse wavelet process has been used here because it will transform the signal into time domain rather than the combination of time and frequency domain.
5. *Watermark extraction process:* The shared key value, scrambling matrix, and the steganography levels vector are used to extract the secret bits from the watermarked ECG signal. Firstly, 32 sub-bands are obtained by applying 5-level wavelet packet decomposition. Next, the secret bits are obtained with the

help of shared key and scrambling matrix according to row sequence fetched from scrambling matrix.

3. **Authentication:** Authentication is a process that ensures that only legitimate users have access to the information. For telemedicine, this is an important issue because sensitive medical data in wrong hands can do a lot of damage. It can also result in lack of trust by patients in telemedicine services, this trust issue is not properly dealt with till now [4]. Many approaches have emerged over the years that have tried to deal with the issue of authentication. Kong *et al.*, have provided a combined approach that has multiple levels of authentication [11]. In this paper, the authors consider signal alteration as a breach of authentication. The authors have used 3 watermark methods (patchwork, LSB, quantization methods) for electroencephalogram (EEG) signal authentication, subjected to several kinds of communication channel errors that are usually encountered. Zan *et al.*, provide us with the issues we have to deal with if we use watermarking for providing authentication [13]. For *e.g.*, as the image is compressed for transmission it may cause watermark destruction, whether to provide complete authentication or content authentication, the watermark should be reversible or permanent, also we have to find a balance between robustness, invisibility and capacity of the watermark. Perminov *et al.*, have compared the information-based (in this the user remembers some information which is later on used for authenticating him, for *e.g.*, username and password in windows), property-based (in this a special device is used is used for authentication, for *e.g.*, smart cards *etc.*), biometric-based (in this user himself is the password, for *e.g.*, iris scanner, fingerprint scanner *etc.*,) authentication methods and decide to avoid these complex methods [14]. Authors have proposed a simple authentication method based on the use of passwords. They provide strength to password method by using counting method which instructs the user to recover the password if the user fails to provide correct password in specified threshold attempts. Authors further increase this method's strength by storing the network address of the attempting user which is used later for identifying the attacker (if suspected that attempting user was an attacker). Pushpa *et al.*, have provided authentication using various watermarking techniques applied to medical images stored on the PACS (Picture Archiving and Communication Systems) [15]. Raman *et al.*, have used a method that uses pin protected smart cards for identification and authentication [16]. Lu *et al.*, give us a whole new perspective of authentication by defining it in terms of access control. The approach taken by the author adds to the features of existing Role Based Access Control (RBAC), the features of rule-based access control module that is based on the classical Flexible Authorization Framework (FAF) model [17]. Starren *et al.*, have divided the network into 2 domains and then use a number of different security solutions, including: UserID and Password, Public Key Infrastructure (PKI) certificates, time-based tokens, filtering based on IP addresses (IP filtering), virtual private networks (VPNs), symmetric and asymmetric encryption schemes, firewalls and dedicated connections [18].

2.2. Visual Cryptography

Naor and Shamir gave the concept of Visual Cryptography (VC) in 1995 [7]. In VC, we generate some shares of the original image and send these shares to some person or a number of persons where they overlap the shares to get an image similar to the original one that represents information of the original image. The shares are just random noise when seen separately. When referring to shares we mean that different components of the original image such that anyone does not reveal any information about the image. The information can only be revealed if the minimum number of required shares are combined through a mechanical process. We consider some assumptions for the VC definition as below:

Assumptions: Suppose we have a binary image which we want to share to n users. k out of n users together can get back original image by overlapping at-least k shares. Let $P(P_1, P_2,.....P_n)$ be set of users which are decomposed into 2 disjoint sets say P_{Auth} and P_{Forbid} where P_{Auth} and P_{Forbid} stands for a set of authorized and unauthorized users respectively. We encrypt the original image I_{orig} into n shares, each P_i receiving exactly 1 or no share. The performance of the scheme depends upon 2 parameters *i.e.*, pixel expansion denoted by m which is the number of pixels (often called sub-pixels) in the shares used to represent the pixel in the original image I_{orig}, and contrast α which is the difference between a black and a white pixel in the encrypted image. Each pixel in I_{orig} is transformed into m sub-pixels, for each n shares. A boolean matrix X of size nxm is used for representing the sub-pixels where value 0 represents a black sub-pixel and value 1 represents a white sub-pixel. Let x_i be the i^{th} row of matrix X where i =1, 2, 3......., n containing sub-pixels for the i^{th} share. Let H(w) be the hamming weight of vector w corresponding to the visual intensity of m where $w = OR(x_{i1}, x_{i2}......x_{ik})$ and $x_{i1}, x_{i2},.........,x_{ik}$ are the rows of the matrix X.

Definition: Assume (P_{Auth}, P_{Forbid}) be an access set for n-users. C_0 and C_1 be 2 collections of nxm boolean matrices (C_0 for black pixel processing and C_1 for white pixel processing), m denoting pixel expansion if there exist contrast, α and threshold (th) for every $P_i \epsilon P_{Auth}$ satisfying the below:

i. Contrast Condition: Any subset $S \epsilon P_{Auth}$ can get back original image I_{orig} by stacking respective shares. More formally, for $X \epsilon C_j$, [j = 0, 1], the row vector $w_j(S, X) = OR\ (x_{i1}, x_{i2}, ...x_{ik})$. Also $H(w_0(S,X)) \leq th\text{-}\alpha(m)$, where m is the size of 1 pixel expansion and $\forall m \epsilon C_0$ and $H(w_1(S,X)) \geq th\ \forall m \epsilon C_1$ where α(m) is the contrast of the reconstructed image and th is the threshold to determine the pixel being black or white.

ii. Security Condition: Any $S \epsilon P_{Forbid}$ can't interpret the original secret image.

When $m=2^{e-1}$ and $\alpha=1/2^{e-1}$, VC Scheme is e out of e, where e = total number of shares created. The 2 out of 2 VC scheme can be solved using 2 sub-pixels per pixel in the original image but this can alter the original image's aspect ratio, so 4 sub-pixels are used. Thus pixel expansion occurs in VC which is quite challenging during implementation. Below is the implementation output of 2 out of 2 VC scheme.

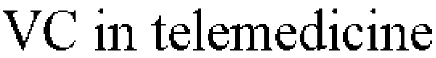


Figure 1. Original Image

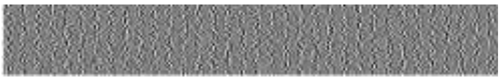


Figure 2. Share 1

Figure 3. Share 2

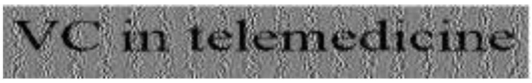


Figure 4. Output of Overlapping Share 1 & Share 2

Out of the original image in Figure 1 we generate 2 shares in Figure 2 and Figure 3. For decryption share 1 and share 2 are overlapped using bitwise OR operation and we get original image's information as in Figure 4.

Naor and Shamir generalized their VC scheme to K out of n scheme in which n shares are made of the original image I_{orig}, requiring at-least k of them to get back I_{orig} from the shares [7]. They also proposed 2 extensions of their scheme: 1. Using continuous tone image (grayscale image) and 2. Based on superimposing images that conceal the existence of secret message [7]. Dipawali *et al.*, suggest a version of VC in which the original image is converted into gray-scale (if color image), then the image is sliced into multiple images (slicing can be done on image either vertically or horizontally but not both), then each sliced image is encrypted using different encryption factor, then cover image is added to increase clarity and thus finally we get multiple encrypted slices [19]. Shah and Gunasekaran apply the concept of VC to provide data privacy while retrieving information on the cloud. The data stored in the cloud is encrypted after applying VC on it, query user poses to retrieve the data is also encrypted [20]. The traditional VC scheme can be used to share only 1 secret image at a time but Bin Yu *et al.*, extends VC so that it can be used to share multiple secrets at a time. To achieve multiple secret's share, the author has constructed base matrices by concatenating submatrices [21]. Shuo-Fang *et al.*, further improves VC scheme by adding a mechanism which ensures the genuineness of generated shares [22]. Shivendra and Sunita propose Verifiable Progressive VC scheme based on verifying the genuineness of shares, improving the quality of the deciphered image with the increasing number of shares. It also solves the problem of pixel expansion, a limit on the number of users/participants and can also effectively localize the tampered region of the share [23].

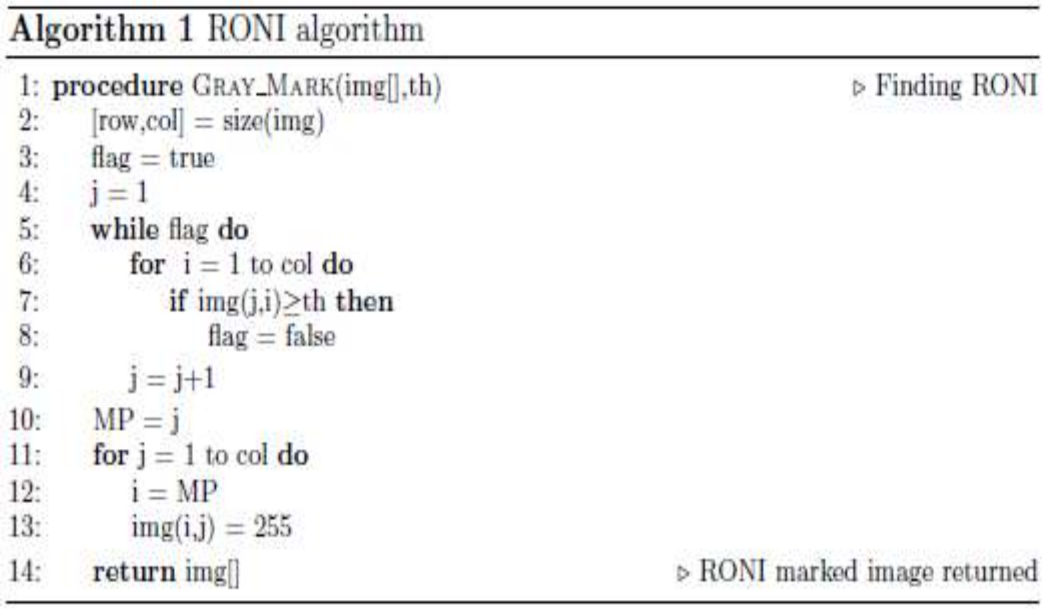
Table 1. Existing Techniques

S.No.	Author Name	Year	Techniques	Type of Data	Result	Remarks
1.	Xuan Kong, Rui Feng [12].	2001	Patchwork, LSB & quantization watermarking methods.	Medical signals	Patchwork method performs better than others when bit error rate in the communication channel is moderate	Authentication achieved using the method
2.	Coatrieux et al.	2002	Non-Blind techniques	Medical images	Modification detection, location, integrity analysis.	Integrity analysis not good.
3.	Hui Huang	2011	Blind & non-blind techniques	Medical images	Solves integrity analysis	Improved & better results than Coatrieux in integrity analysis.
4.	Basant Kumar, Harsh Vikram Singh, Surya Pal Singh, and Anand Mohan	2011	Spread Spectrum Watermarking	Medical Images	Authentication, integrity and confidentiality can be achieved	Susceptible to problems related to watermarking
5.	Shifali Arora, Jennifer Yttri, & Wendy Nilsen	2014	passwords, communication over secure VPN(virtual private network) connection, use of encrypted information etc.	Medical data.	Simple protection and encryption achieved	Basic privacy protection in mHealth
6.	L.Keerthana, B.Venkataramanaiah	2014	Ecg Steganography based watermarking	Medical data	Watermarked Ecg signals obtained.	Privacy protection for medical data.

3. Proposed Approach

In our work, we have proposed an algorithm using VC to ensure the security of telemedicine transaction. Security may be of authenticity, privacy, or integrity. The primary concern of our information base is image data like X-ray, MRI, CT-scan etc. for the purpose of transferring patient's information for diagnosis. Following are the basic steps in order to ensure the security of the image:

1. Converting the image to grayscale image (if a colour image).
2. Finding and marking the RONI (region of non-interest) in the image.
3. Finding digest of some portion of the image (for integrity check).
4. Embedding signature (unique) information like Patient ID, name etc. along with digest in RONI.
5. Creating shares of embedded RONI.



Algorithm 1 RONI algorithm

```
procedure GRAY_MARK(img[],th)                    ▷ Finding RONI
    [row,col] = size(img)
    flag = true
    j = 1
    while flag do
        for  i = 1 to col do
            if img(j,i)≥th then
                flag = false
        j = j+1
    MP = j
    for j = 1 to col do
        i = MP
        img(i,j) = 255
    return img[]                                 ▷ RONI marked image returned
```

Algorithm 1 RONI, takes as input a grayscale image, threshold (th), and outputs an image that has RONI marked in the top part of the image. To do so first the total number of rows and columns are find out, then we set a flag to true and a variable j = 1. Now we loop until the flag is false. Inside the loop, we go from the first column to the last checking if there exists a pixel value at a location marked by row and column number that is greater than some threshold value. After experimenting on a number of images, the threshold was found to be having value 22. On finding such pixel value we set the flag to false thus terminating the loop, otherwise, we increment the value of variable j. After the loop terminates we have got ourselves the row number j that we call mark point (MP) which is then used to mark a horizontal white line across the image representing the separation between ROI and RONI. Similarly, we can mark bottom, left, right RONI with minor modifications in the above algorithm. Figure 5 and Figure 6 shows the result of the implementation of the above algorithm on a grayscale image.

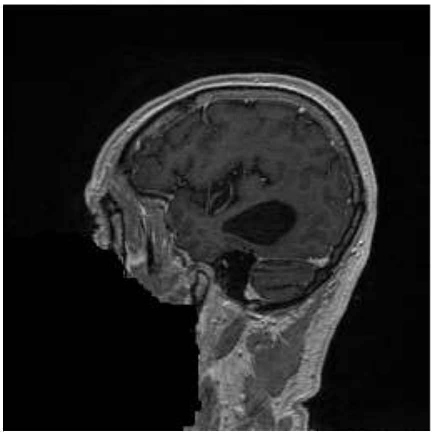


Figure 5. Unmarked Original Image [25]

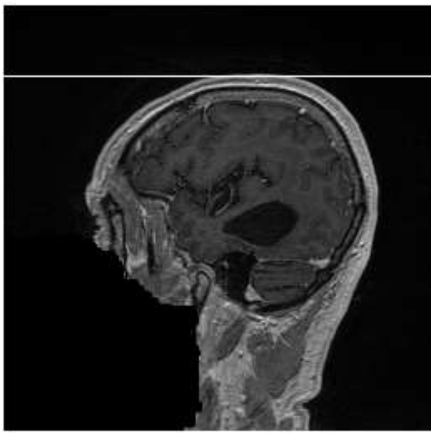
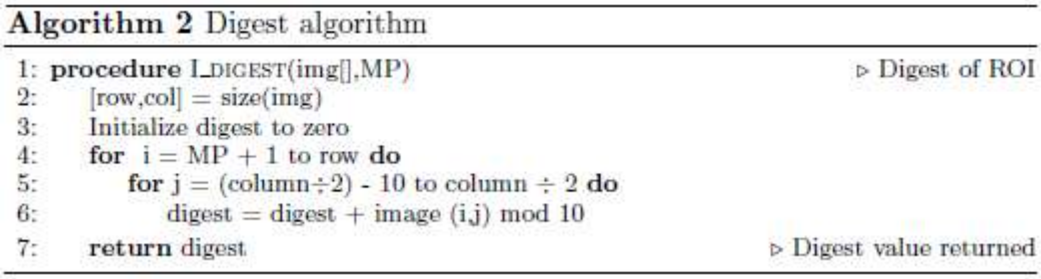


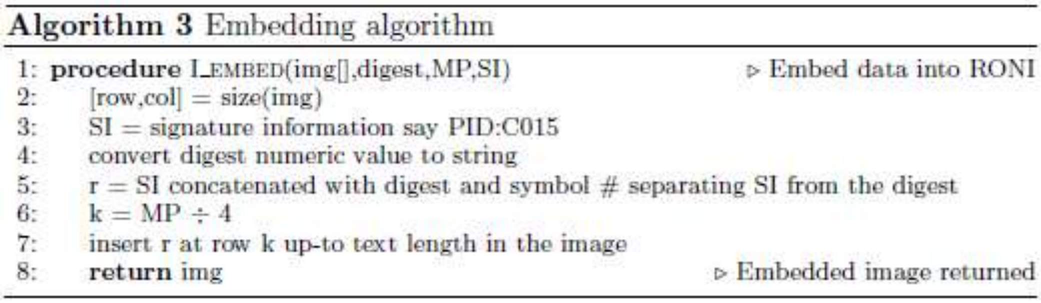
Figure 6. Marked Original Image



Algorithm 2 Digest algorithm

```
procedure I_DIGEST(img[],MP)                                    ▷ Digest of ROI
    [row,col] = size(img)
    Initialize digest to zero
    for i = MP + 1 to row do
        for j = (column÷2) - 10 to column ÷ 2 do
            digest = digest + image (i,j) mod 10
    return digest                                               ▷ Digest value returned
```

Algorithm 2 Digest, takes as input an image and mark point (MP) obtained from RONI algorithm and outputs the digest value of the image. When referring to digest we mean, calculating a numeric value by performing some operation on pixel values of an image. To do so, we first initialize variable digest to 0. Then we iterate over rows and columns with rows starting from 1 greater than mark point MP up to the last row, and columns from half less than 1 to half. While iterating we do the sum of digest and value of the pixel at that row, column number modulo 10. Then this sum is stored in the variable digest which is returned as output.



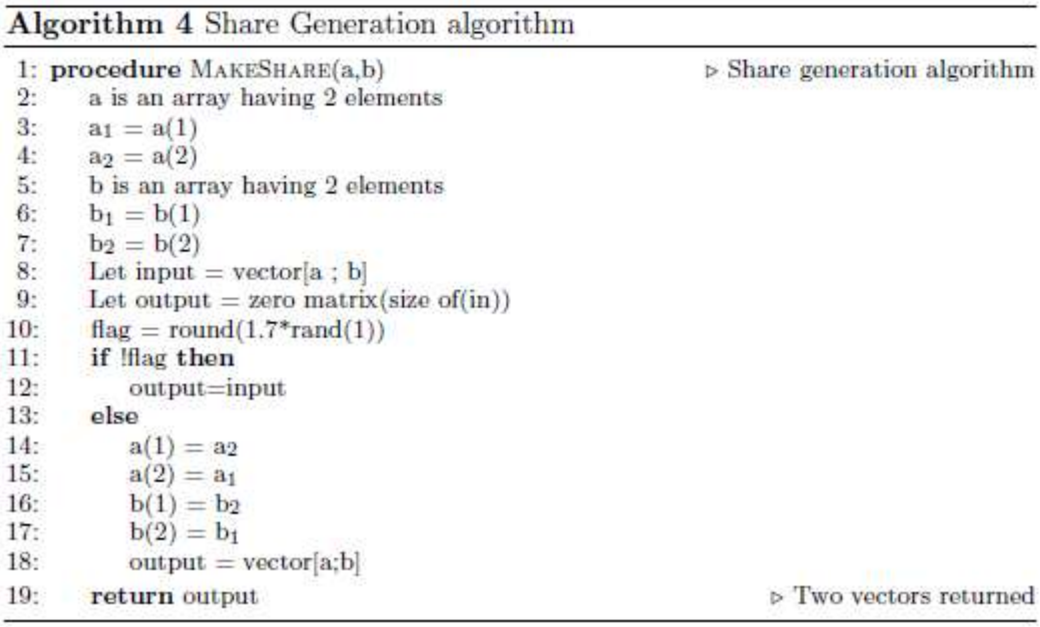
Algorithm 3 Embedding algorithm

```
procedure I_EMBED(img[],digest,MP,SI)                           ▷ Embed data into RONI
    [row,col] = size(img)
    SI = signature information say PID:C015
    convert digest numeric value to string
    r = SI concatenated with digest and symbol # separating SI from the digest
    k = MP ÷ 4
    insert r at row k up-to text length in the image
    return img                                                  ▷ Embedded image returned
```

Algorithm 3 Embedding, takes an image, signature information (SI), digest value (obtained from algorithm I_digest), mark point (obtained from Gray_Mark algorithm) as inputs and outputs as an embedded image. To get the embedded image, we firstly convert numeric digest value to data type string (conversion is done by considering numeric data as a numeric array and converting it to character array), combine signature information with converted digest and symbol # inserted between SI and digest separating them and store it in variable r. Then the algorithm calculates (MP÷4) to position it somewhere at middle row-wise in the marked region in the image and assign it to variable k which is

used as a location for inserting r into the image. Finally, we insert the value of r at location k in the image up to the length of r.

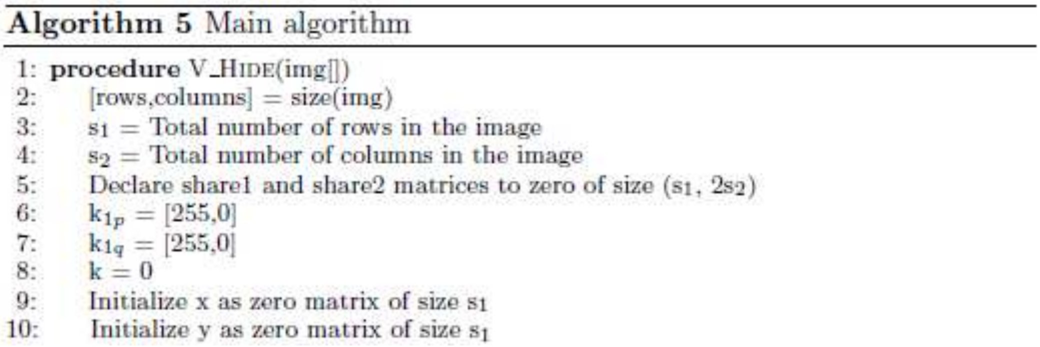
We have proposed an algorithm using the fundamental concept of VC for the grayscale image. In this original pixel of the patient's signature are converted into s sub-pixels. The algorithm converts pixel into sub-pixels in such a way that it creates n set of s. This n set represents n different shares. In this algorithm value of s and n are 2. The shares are transmitted on the network to different responsible authority that ensures authentication and privacy during decryption of message without computation algorithm. Here decryption is a mechanical process in which shares are overlapped to get secret information. The proposed algorithm is defined in 2 parts: 1. Generation of shares using MakeShare 2. Visual Encryption using V_Hide.



Algorithm 4 Share Generation algorithm

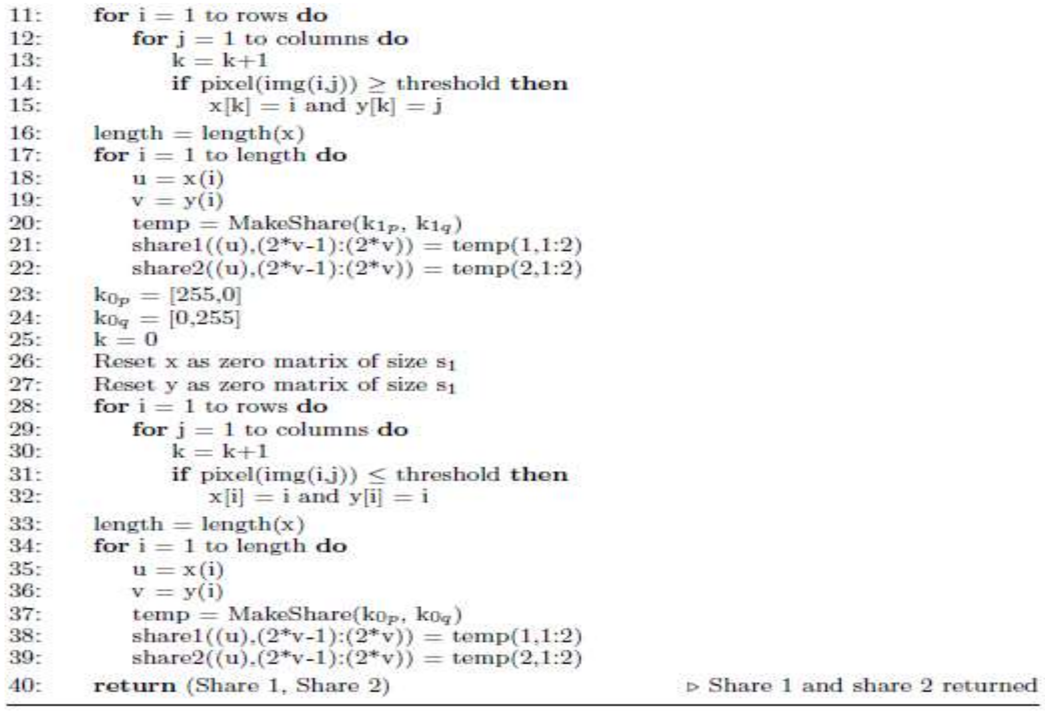
```
procedure MakeShare(a,b)                              ▷ Share generation algorithm
    a is an array having 2 elements
    $a_1$ = a(1)
    $a_2$ = a(2)
    b is an array having 2 elements
    $b_1$ = b(1)
    $b_2$ = b(2)
    Let input = vector[a ; b]
    Let output = zero matrix(size of(in))
    flag = round(1.7*rand(1))
    if !flag then
        output=input
    else
        a(1) = $a_2$
        a(2) = $a_1$
        b(1) = $b_2$
        b(2) = $b_1$
        output = vector[a;b]
    return output                                     ▷ Two vectors returned
```

Algorithm 4 Share Generation, takes as input 2 arrays a and b containing 2 values each. It then randomly assigns values to a resultant vector output depending upon the values of the flag and returns this vector.



Algorithm 5 Main algorithm

```
procedure V_Hide(img[])
    [rows,columns] = size(img)
    $s_1$ = Total number of rows in the image
    $s_2$ = Total number of columns in the image
    Declare share1 and share2 matrices to zero of size ($s_1$, $2s_2$)
    $k_{1p}$ = [255,0]
    $k_{1q}$ = [255,0]
    k = 0
    Initialize x as zero matrix of size $s_1$
    Initialize y as zero matrix of size $s_1$
```



```
11:  for i = 1 to rows do
12:      for j = 1 to columns do
13:          k = k+1
14:          if pixel(img(i,j)) $\geq$ threshold then
15:              x[k] = i and y[k] = j
16:  length = length(x)
17:  for i = 1 to length do
18:      u = x(i)
19:      v = y(i)
20:      temp = MakeShare($k_{1_p}$, $k_{1_q}$)
21:      share1((u),(2*v-1):(2*v)) = temp(1,1:2)
22:      share2((u),(2*v-1):(2*v)) = temp(2,1:2)
23:  $k_{0_p}$ = [255,0]
24:  $k_{0_q}$ = [0,255]
25:  k = 0
26:  Reset x as zero matrix of size $s_1$
27:  Reset y as zero matrix of size $s_1$
28:  for i = 1 to rows do
29:      for j = 1 to columns do
30:          k = k+1
31:          if pixel(img(i,j)) $\leq$ threshold then
32:              x[i] = i and y[i] = i
33:  length = length(x)
34:  for i = 1 to length do
35:      u = x(i)
36:      v = y(i)
37:      temp = MakeShare($k_{0_p}$, $k_{0_q}$)
38:      share1((u),(2*v-1):(2*v)) = temp(1,1:2)
39:      share2((u),(2*v-1):(2*v)) = temp(2,1:2)
40:  return (Share 1, Share 2)                    ▷ Share 1 and share 2 returned
```

The objective of algorithm 5 Main, is to create two shares for a given image where each share does not reveal any relevant information about the original image. In order to generate the shares, the algorithm first finds the size of the original image and declares two zero matrices of the same size as of the original image, respectively for share 1 and share 2. In third and fourth step, two vector variables have been declared having values 255 and 0 respectively. In the fifth step, the algorithm scans each pixel of the image and finds the pixels whose value is greater than a defined threshold (th) and assigns the row and column number of the pixel into two vectors x and y respectively. After experimenting on a number of images, the threshold was found to be having value 22. Step 6 finds the total number of elements in vector x and for each value of x, the algorithm assigns to variables a and b two values x and y of the corresponding index. In the next step, temp matrix is defined by MakeShare function. Share 1 and Share 2 are defined by temp corresponding to the index u and v. In step 8 to 12 the above process of assignment of values to the shares are done for all those pixels whose values are less than the threshold. In the end, we have got two shares i.e. Share 1 and Share 2 having a similar size as the original with the same number of rows but double the columns.

In the medical image, to maintain the size of the original image in the share we only take the half size of the RONI where patient information is embedded. After the creation of shares, its size doubles (number of columns becomes twice), making the resultant number of columns in share equal to the original image. This process of considering half of the RONI maintains the aspect ratio of the generated share image.

How our approach achieves Authentication, Privacy and Integrity?

Authentication: We embed signature information (SI) such as patient ID (PID) *etc.*, which is used for verification of particular patient's information at the receiver end. For *e.g.*, if sender embeds PID: C015 then applies VC and sends it to a receiver and the receiver finds PID: C015 upon combining shares then it means that the information is authentic and the image can be used.

Privacy: By applying VC we generate shares of RONI and require a minimum number of shares to reveal the information. The individual shares are just noise and do not deliver any information when analyzed individually, making the ROI of the image a random image like the one available on the internet. Thus without the information in RONI region, no one can know that the image in ROI belongs to whom making shares as the means of providing privacy protection of telemedicine data.

Integrity: To achieve the goal of integrity verification we calculate the digest of a portion of the image which is then embedded along with SI with # as a separator. At the receiving end, the receiver recalculates the digest using the same algorithm and compares it with the embedded digest value received (the value after # separator). If both are same then the image is intact otherwise some modification has been done.

4. Performance Analysis and Results

4.1 Performance Analysis

The performance of the approach has been analyzed using below metrics [24]:

1. **MSE (Mean Square Error):** It calculates mean-squared error between two image arrays.

$$MSE = \frac{1}{m \times n}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(I^{'}(i,j) - I(i,j)\right)^{2}$$

Here I = reference image, $I^{'}$ = image to be compared.

2. **RMSE (Root Mean Square Error):** It is the square root of mean-squared error.

$$\mathrm{RMSE} = \sqrt{MSE}$$

3. **PSNR (Peak Signal-To-Noise Ratio):** It calculates peak signal-to-noise ratio for an image with respect to a reference image.

$$PSNR = 20\log_{10}\left(\frac{255}{RMSE}\right)$$

4. **SSIM (Structure Similarity Index Map):** It compares luminance, contrast and structure of two different images. It can be treated as a similarity measure of two different images.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1) \times (2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1) \times (\sigma_x^2 + \sigma_y^2 + C_2)}$$

Here μ_i = mean intensity, σ_i = standard deviation, i = x or y and C_i = constant to avoid instability when $\mu_x^2 + \mu_y^2$ approaches zero which equals $C_i = (k_i,L)^2$, where $k_i << 1$ and L = dynamic range of pixel values *e.g.*, L = 255 for 8-bit greyscale image.

Table 2 shows the result of the application of these metrics onto the proposed approach using Figure7 and Figure 10.

Table 2. Performance Analysis

S.No.	Metric	Result
1.	MSE	4.2576e+03
2.	RMSE	65.2504
3.	PSNR	11.8391
4.	SSIM	0.8933

4.2. Results

We have used DICOM images obtained from [25] as input image since it is the international standard for sharing medical images. We have used Matlab R2017a for the implementation.

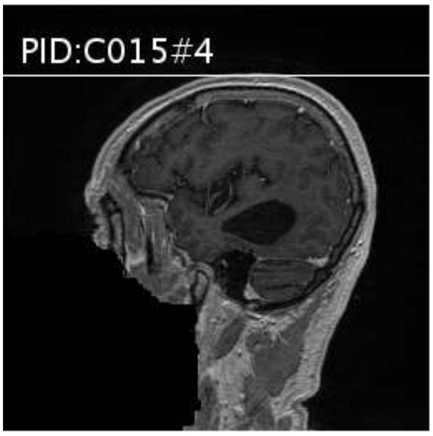


Figure 7. Original Secret Image [25]

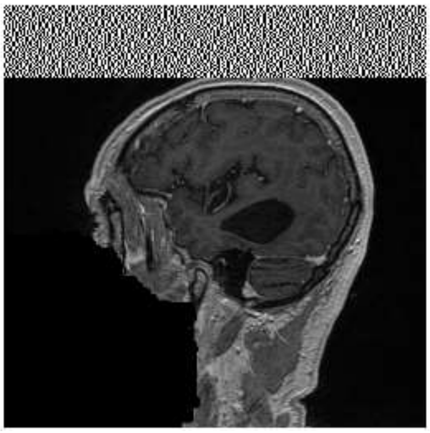


Figure 8. Share 1

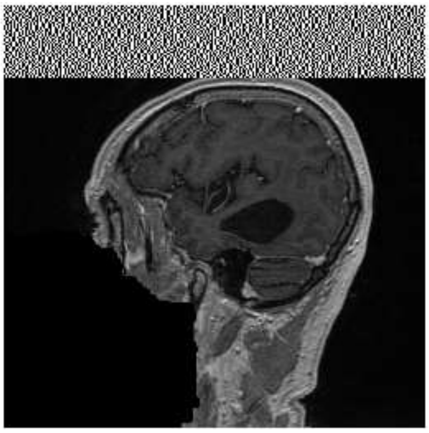


Figure 9. Share 2

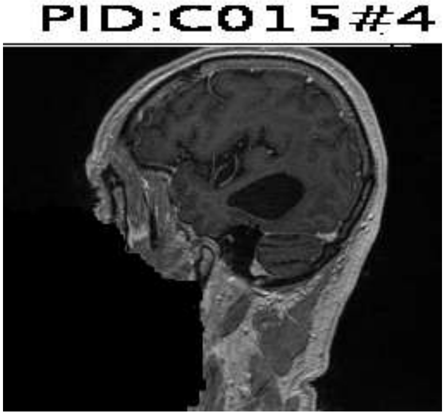


Figure 10. Output of Overlapping Share 1 and 2

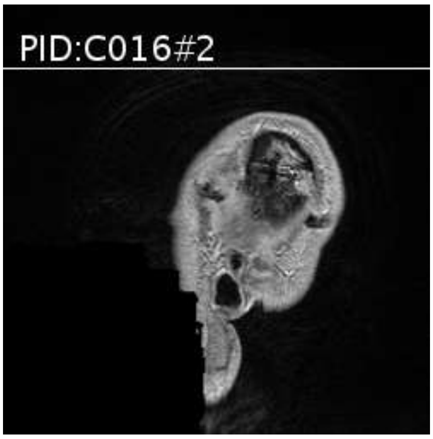


Figure 11. Original Secret Image [25]

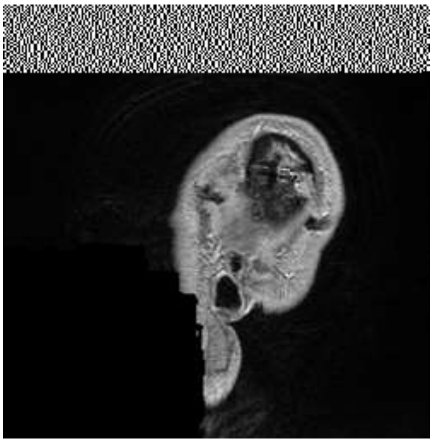


Figure 12. Share 1

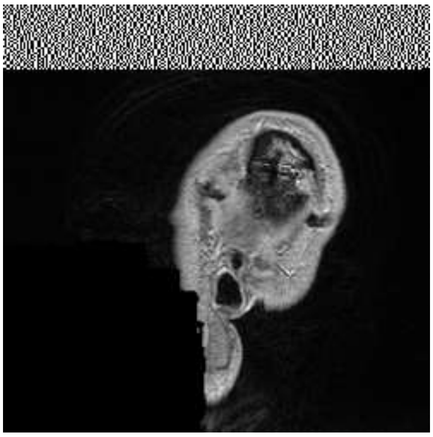


Figure 13. Share 2

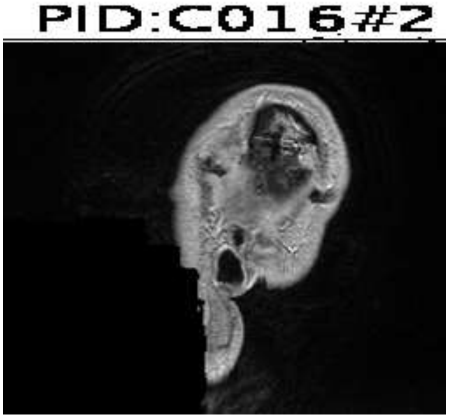


Figure 14. Output of Overlapping share 1 & 2

MRI image in Figure 7 and Figure 11 contains patient's signature and image digest value in the left half of RONI. Proposed system creates two transparent shares for an original image. Share 1 is created for RONI that represents expanded pixels into the double of its column size as in Figure 8 and Figure 12. Share 2 also represents the same type of information as shown in Figure 9 and Figure 13. For decryption of patient's signature information and digest value share 1 and share 2 are overlapped and decrypted information is shown in Figure 10 and Figure 14. The visual perception of decrypted information is quite good and all the letters are clearly visible.

In our approach, we utilize Visual Cryptography to secure images used in telemedicine to provide a secure environment for information exchange. While performing Visual Cryptography operation on an image we apply it only to a specific region that contains information of least interest thus keeping the information of interest untouched. There are many existing techniques that try to provide security to telemedicine data like watermarking, encryption etc. but these are complex techniques requiring some time for encryption & decryption. Moreover, they are vulnerable to attacks like brute force etc. in which encryption key can be compromised. In contrast to these techniques, our VC approach has constant decryption complexity.

5. Conclusion & Future Scope

5.1. Conclusion

In telemedicine, challenging part was making patient confident about the security of data like medical images, personal details *etc*. When we use a public network then it becomes even more crucial. In this article, we have provided the solution to security issues such as authentication, privacy and integrity using VC. All the existing solutions for this problem were either defined by watermarking or image encryption algorithms which have the possibility of being compromised. VC based solutions create more than 1 shares of the given data that has random information making it impossible to decode. These different shares are then sent to different responsible authorities via different channels which reduces the possibility of an attack on all the channels simultaneously. If all responsible authorities agree then they can decrypt the message by overlapping the shares (in XOR fashion), one over the another with mechanical process resulting in $\theta(1)$ complexity. The proposed algorithm for grayscale image creates 2 shares and overlapping of these shares (in XOR fashion) clearly depicts the patient's information that was presented in the original image. This algorithm ensures authentication at the receiver end, the integrity of the image via digest value and also about the privacy of the patients' data.

It is quite efficient due to the mechanical process of decryption. The proposed algorithm has performance metrics as MSE (mean square error), RMSE (root mean square error), PSNR (peak signal-to-noise ratio) and SSIM (structure similarity matrix) having values 4.2576e+03, 65.2504, 11.8391 and 0.8933 respectively.

5.2. Future Scope

VC is a better solution for telemedicine security when more than 1 authority is available at the telemedicine centre or a single authority is in a different role. The proposed algorithm has an expansion of pixels that can be solved in future for medical data of different formats (MRI, ultrasound, X-Ray etc.). There are some other challenges in telemedicine security solution using VC such as randomness, accountability and physical security.

References

[1] M. Kay, J. Santos and M. Takane, “Telemedicine: opportunities and developments in Member States: report on the second global survey on eHealth. Global Observatory for eHealth Series”, WHO Geneva, vol. 2, **(2010)**.

[2] Overcoming 4 Challenges in Implementing Telemedicine, Healthcare's Next Frontier (2012) Becker's Helath IT & CIO Report.

[3] H. Huang, “Contribution to the control of the integrity of medical images”, TELECOM-Bretagne, Brest, France, **(2011)**.

[4] V. Garg and J. Brewer, “Telemedicine Security: A Systematic Review”, Journal of Diabetes Science and Technology, DOI: 10.1177/193229681100500331, vol. 5, no. 3, **(2011)**, pp. 768-777.

[5] S. Das and A. Mukhopadhyay, “Security and Privacy Challenges in Telemedicine”, CSI Communications, vol. 35, **(2011)**.

[6] R. Gupta, R. S. Gamad and P. Bansod, “Telemedicine: A brief analysis”, Cogent engineering, DOI: 10.1080/23311916.2014.966459, **(2014)**.

[7] M. Naor and A. Shamir, “Visual cryptography”, Proceedings of Advances in Cryptology - Eurocrypt, DOI: 10.1007/BFb0053419, **(1994)**, pp. 1-12.

[8] J. G. Hodge, L. O. Gostin and P. D. Jacobson, “Legal Issues Concerning Electronic Health Information: Privacy, Quality, and Liability”, The Journal of the American Medical Association, DOI: 10.1001/jama.282.15.1466, vol. 282, no. 15, **(1999)**, pp. 1466-1471.

[9] C. M. Rackett, “Telemedicine Today and Tomorrow: Why “Virtual” Privacy Is Not Enough”, Fordham Urban Law Journal, vol. 25, no. 1, **(1997)**.

[10] S. Arora, J. Yttri and W. Nilsen, “Privacy and Security in Mobile Health (mHealth) Research”, Alcohol Research, vol. 36, no. 1, **(2014)**, pp. 143-151.

[11] L. Keerthana, B. Venkataramanaiah and E. Mennigen, “Ecg Steganography Based Privacy Protection of Medical Datas for Telemedicine Application”, IOSR Journal of VLSI and Signal Processing, vol. 4, no. 2, **(2014)**, pp. 46-51.

[12] X. Kong and Rui Feng, “Watermarking medical signals for telemedicine”, IEEE Transactions on Information Technology in Biomedicine, DOI: 10.1109/4233.945290, vol. 5, no. 3, **(2001)**, pp. 195-201.

[13] J. Zain and M. Clarke, “Security in Telemedicine: Issues in Watermarking Medical Images”, Sciences of Electronic, Technologies of Information and Telecommunications, Tunisia, **(2005)**.

[14] V. V. Perminov, V. E. Antciperov, D. S. Nikitov and S. A. Nikitov, “Preventing Unauthorized Access to User Accounts in a Telemedicine Consultation System”, Journal of Communications Technology and Electronics, DOI: 10.1134/S1064226909110138, vol. 54, no. 11, **(2009)**, pp. 1319-1321.

[15] K Pushpala and R Nigudkar, “A Novel Watermarking Technique for Medical Image Authentication”, Computers in Cardiology, DOI: 10.1109/CIC.2005.1588194, **(2005)**.

[16] R. S. Raman, R. Reddy, V. Jagannathan, S. Reddy, K. Joseph Cleetus and K. Srnivas, “A Strategy for the Development of Secure Telemedicine Applications”, Proceedings of the American Medical Informatics Association, **(1997)**, pp. 344-348.

[17] S. Lu, Y. Hong, Q. Liu, L. Wang and R. Dssouli, “Access control in e-Health portal systems”, Proceedings of the International Conference on Innovations in Information Technology, DOI: 10.1109/IIT.2007.4430378, **(2007)**, pp. 88-92.

[18] J. Starren, S. Sengupta, G. Hripcsak, G. Ring, R. Klerer and S. Shea, “Making Grandma's Data Secure: A Security Architecture for Home Telemedicine”, Proceedings of the American Medical Informatics Association, **(2001)**, pp. 657-661.

[19] D. Gabhane, S. Gupta, R. Rajgure, P. Verma, D. Mande and S. Phiroj, “Visual Cryptography: An Efficient Technology for Securing Data”, International Journal of Computer Science and Mobile Computing, vol. 5, no. 3, **(2016)**, pp. 776-781.

[20] H. Ram Sah and G. Gunasekaran, "`Preserving Data Privacy with Record Retrieval using Visual Cryptography and Encryption Techniques", Indian Journal of Science and Technology, DOI: 10.17485/ijst/2016/v9i32/88703, vol. 9, no. 32, **(2016)**.

[21] B. Yu, X. Xu and L. Fang, "Multi-secret sharing threshold visual cryptography scheme", Proceedings of the International Conference on Computational Intelligence and Security Workshops, DOI: 10.1109/CISW.2007.4425620, **(2007)**, pp. 815-818.

[22] S.-F. Hsu, Y.-J. Chang, R.-Z. Wang, Y.-K. Lee and S.-Y. Huang, "Verifiable Visual Cryptography", Proceedings of the sixth International Conference on Genetic and Evolutionary Computing, DOI: 10.1109/ICGEC.2012.150, **(2012)**, pp. 464-467.

[23] S. Shivani and S. Agarwal, "VPVC: verifiable progressive visual cryptography", Pattern Analysis and Applications, DOI: 10.1007/s10044-016-0571-x, vol. 21, no. 1, **(2018)**, pp. 139-166.

[24] R. Srivastava, "Performance Measurement of Image Processing Algorithms", Professor, Department of Computer Science & Engineering, IIT BHU, India.

[25] K. Clark, B. Vendt, K. Smith, J. Freymann, J. Kirby, P. Koppel, S. Moore, S. Phillips, D. Maffitt, M. Pringle, L. Tarbox and F. Prior, "The Cancer Imaging Archive (TCIA): Maintaining and Operating a Public Information Repository", Journal of Digital Imaging, DOI: 10.1007/s10278-013-9622-7, vol. 26, no. 6, **(2013)**, pp. 1045-1057.

Authors

Arvind Bakshi: Arvind Bakshi is currently pursuing his masters in computer engineering at National Institute of Technology, Kurukshetra, Haryana, India. He has completed his bachelors in computer science and engineering from Haryana Engineering College, Jagadhri, Haryana, India. His areas of interest are Image Processing, Cryptography, Data Security.

Anoop Kumar Patel: Anoop Kumar Patel is currently Assistant Professor at National Institute of Technology, Kurukshetra, Haryana, India. He has completed his masters in computer science and engineering from MNIT, Allahabad, UP, India and bachelors in computer science and engineering. His areas of interest are Image Processing, Medical Imaging, Algorithms and Data Structure, Computational theory.