

Secure Medical Image-Sharing Mechanism based on Visual Cryptography in EHR system

Dana Yang*, Inshil Doh**, Kijoon Chae*

* Department of Computer Science and Engineering, Ewha Womans University, Seoul, Korea

** Department of Cyber Security, Ewha Womans University, Seoul, Korea

yangzzzz@ewhain.net, isdoh1@ewha.ac.kr, kjchae@ewha.ac.kr

Abstract— Securely sharing electronic health records (EHR) has attracted attention in medical environment. We discuss critical issues related to EHR-sharing and provide how to share a medical image of EHRs based on visual cryptography(VC) and secret sharing with password of practitioners for convenience in distributed system. Also, our proposal is applied to real system “openEMR” and evaluated in respect of performance and security.

Keywords— secure data management, sharing medical image, visual cryptography, secret sharing

I. INTRODUCTION

Information systems in healthcare industry generally have stored medical data about patients, such as X-ray, MRI scan, CT scan, prevention, diagnosis, treatment of diseases and personalization of health care, in occlusive electronic medical record (EMR) system [1]. Currently, each medical institution has its own database for EMRs and shares those between different EMR systems on internet. It is called EHR system. Almost practitioners of healthcare industry use interchangeably EMR and EHR [2]. However, it is difficult that information between other EMR systems across administrative domains is shared. Also, the interoperation among distributed EMR systems is relatively slow and vulnerable to attacks. The problem can be occurred in situation each other medical institution should urgently share patient data, especially when he or she is fallen into unconsciousness in location far away from his or her residence.

Fig. 1 shows an estimated scenario which can be sufficiently happened in healthcare environment [3]. Suppose each hospital has private EMR database which should not be accessed except for public EHR database [4]. A patient is accurately diagnosed in nearby hospital A. Afterward, the patient may visit certain disease-specialized hospital B for better treatment. The patient can demand sharing information between each hospital for convenience or emergency. In this scenario, prominent issues are securely how to manage the EMRs and communicate with the institutions because the medical data of patient is critical and private. Our proposal provides the scheme to share and manage medical images of patient, based on VC and secret sharing method with password of practitioners. Real EHR environment to develop it has been built using open source “openEMR”. As the result,

it is evaluated by correlation coefficient with original image and reconstructed image in R language, and confirms outstanding performance and security.

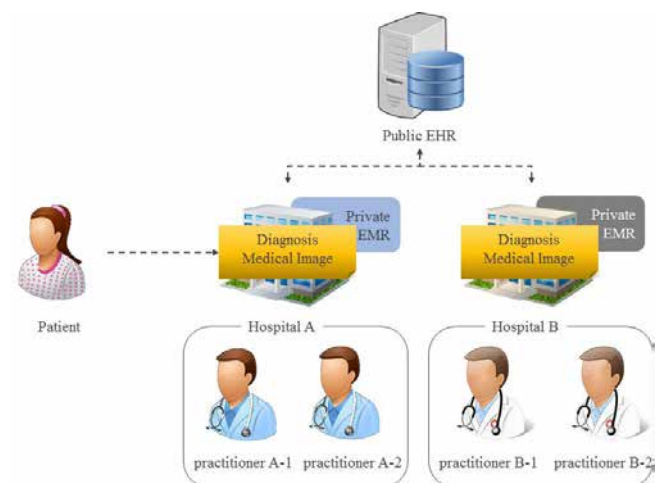


Figure 1. Estimated Scenario

II. RELATED WORKS

Suggested mechanism is based on VC and secret sharing presented by Shamir. Those research and how to apply related research to our mechanism are explained specifically.

A. Visual Cryptography

Founded on image cryptography, VC was announced by Naor and Shamir [5]. The method of encrypting original image into shared images reveals the secret message or image of original image certainly after stacking a sufficient number of shares [6]. In other words, it is to make shared images derived from original image just by converting each pixel to pattern looking like noise or gray [7]. Now we explain concretely basic VC and how to transform VC.

Firstly an original image including secret message has to be prepared. For example, the original image of Fig. 2 involves number “7968” as secret message. The image should be composed of white and black. In fact, researches about VC had been developed to encryption of half-tone moreover color image. But we explain basic VC applied to this paper.

For encryption, some patterns to transform a original image should be prepared. The patterns consist of pixels arranged in a 2×2 array. The half of 4 pixels is filled with black and the rest subpixels become transparent. 6 patterns made according to this rule are two horizontal shape, two vertical shape and two diagonal shape such as second row of Fig. 3. Shared images based on VC is created only with the shapes. Actually VC converts randomly one pixel of original image to one of the shapes and fills whole shared image with the shapes. Then the shared images look like gray in human eyes because the subpixels of the shapes become as noise with random combination of patterns consisting of black and white. However the way to construct the subpixels of background and message in shared image should be adapted to opposite method. If you want to convert a pixel of background in the original image to one of patterns to construct shared image, you should be following to background pixel matrix in Fig. 3. For example, if a background pixel in original image is converted to pattern no 3 decided at random, subpixels of the position in first shared image (share 1 in Fig. 3) should accurately become left-vertical pattern. In case of second shared image, the subpixels of precisely same position should be same pattern. After all background pixels of the both shared images are created according to this process, the background of shared images to be overlapped seem like gray constructed with black and transparent.

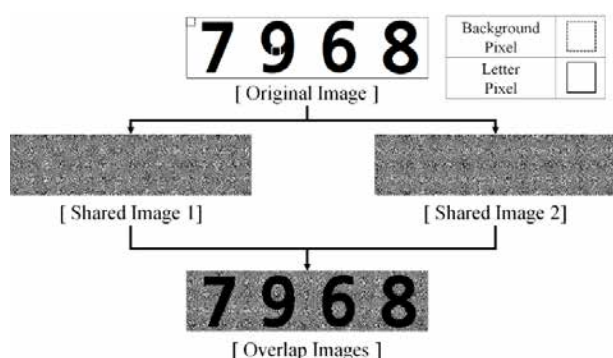


Figure 2. Process to make shared images from original and view secret message

shape no	Background Pixel			Letter Pixel		
	Share1	Share2	overlap	Share1	Share2	overlap
1		+		=		
2		+		=		
3		+		=		
4		+		=		
5		+		=		
6		+		=		

Figure 3. How to make pixel pattern in shared image

Likewise, the message part of shared image is produced in accordance with matrix of message pixel in Fig. 3. If a

message pixel in original image is transformed to diagonal pattern (shape no 5) determined randomly, the subpixel of first shared image should set left-diagonal pattern exactly at the position. Another shared image has to be defined as antitypical shape at the same position. In this way, whole message part of shared images is filled. When the both shared images are correctly stacked up, the pixels of secret message part become black because transparent pixels are superseded by the black of pattern in another shared image and seem as black.

In the conclusion, shared image 1 in Fig. 2 seems gray. Presented on Fig. 2, shared image 2 also appears similar with first shared image. However each shared image never reveals secret message “7968” and any rule to construct the shared image. Exclusively when both shared images are stacked up, the view of human can confirm the message like bottom picture in Fig. 2. If the shared images are not matched from start point to end point or one of shared images is distorted, you cannot view the message at all. The principle is to utilize letter having higher contrast than background. Therefore VC has lower computation for encryption and don’t require any computation for decryption.

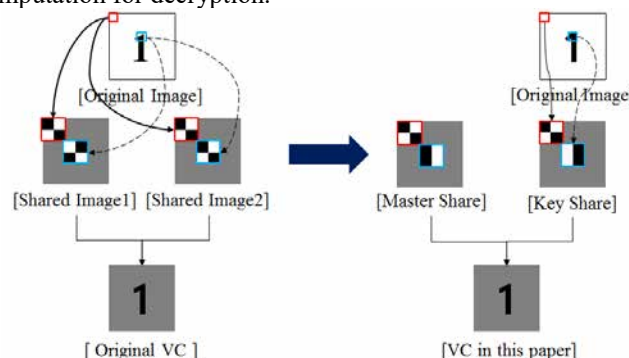


Figure 4. Compare with Basic VC and VC in this paper

Fig. 4 describes process encrypted and decrypted by original VC and by proposal VC in this paper. With SEED, VC used in this paper creates independently shared image 1 called master share (MS). Shared image 2 called key share (KS) is derived by original image. As the result, MS is unrelated to original image and only related with SEED to help VC decide the patterns chosen by random function. Our goal is to produce and manage MS by SEED and KS derived by a medical image.

B. Secret Sharing

Secret Sharing scheme had been presented on title “How to share a secret” based on polynomial features [7]. The main idea is that if users know some k points of n points at least, they can discover the secret. For example, they can get unique linear polynomial line with ‘a’ incline from only 2 points as Fig. 5. Likewise, quadratic polynomial can be ensured by 3 points and cubic curve can be ensured by 4 points. Therefore, if they know k points at least, they can acquire $(k-1)$ degree of polynomial [9]. In practical system, one of participants or group manager possessing secret number S generates random number R . He or she can prepare 1 degree of polynomial ‘ $y=Sx+R$ ’ and send any point passing through the polynomial

to each participant. If participants share own point securely and obtain another point, the participant can verify S. In fact, goal of this scheme is to split one data into some pieces and reconstruct the data easily from collecting some pieces more than threshold. But in this paper, joined EHR or EMR systems already know one point associated with password and share another point. As the result, the systems can share secret.

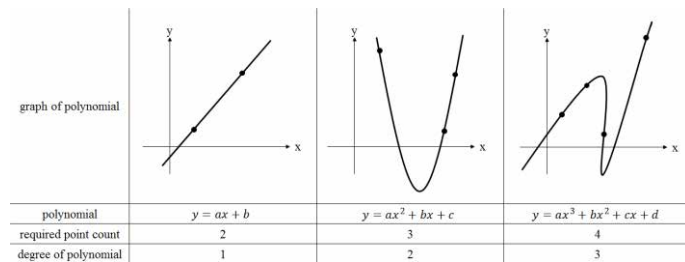


Figure 5. Correlation between required point count and degree about polynomial

III. PROPOSED MECHANISM

Both private EMR system and public EHR system have shared several information of practitioners for authentication and basically patient data. However it is difficult to manage and share the data in various private EHR systems for security danger. We divide registration part and view part about medical image and describe process for those parts with reference to Fig. 1

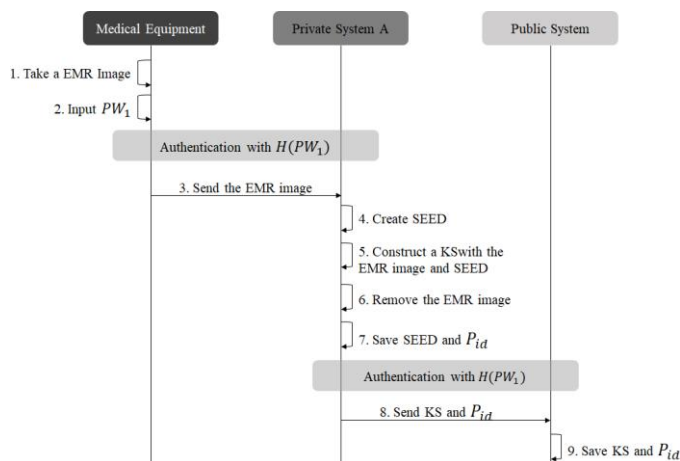


Figure 6. Process for registration of medical image

A. Registration of medical image

Fig 6 shows firstly how to register a medical information of patient into a private system and public system. After a doctor or nurse affiliated in hospital A takes a medical picture of patient as X-ray, the practitioner is authenticated from private EMR system A (PRS_A) by hashing own password ($H(PW_1)$) and sends the picture. Then PRS_A generates a random number SEED, and constructs key share image (KS) based on VC with the picture and SEED. The original picture is removed because the KS includes information about it. It saves SEED and patient ID (P_{id}) to search easily. After the practitioner is authenticated again, he or she sends the key share and P_{id} to

public EHR system (PBS). It receives and saves those data. Eventually SEED and key shared image is saved separately and more securely.

B. View of medical image

After registration process, Fig. 7 shows firstly how to obtain the information of SEED and KS about the medical image and view the reconstructed image.

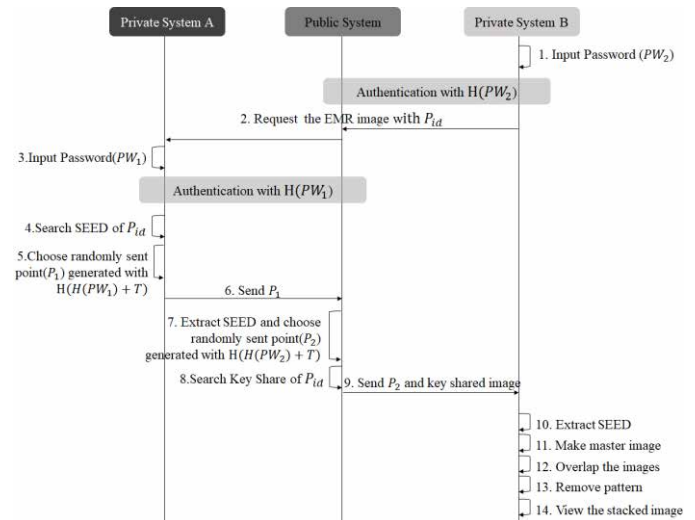


Figure 7. Process for view of medical image

Engaged in hospital B, A doctor who wants the medical image of patient inputs own password (PW_2) to private system B. After authentication with hashing PW_2 , the private system requests the image with P_{id} to PRS_A via PBS . Then, one of practitioners in PRS_A confirms the request and inputs own PW_1 for approval. After authentication with $H(PW_1)$, it searches SEED associated with P_{id} . For linear polynomial, it defines one point to be created by hashing value to add current time (T) to $H(PW_1)$. Actually one point is composed of 2 values (x coordinate and y coordinate), but hash result is one value having fixed length, 256 bits or 512 bits [10]. We stipulate prefixed half of hash is x coordinate and the rest is y coordinate. The linear polynomial is made by drawing incline as SEED over passing through the point. PRS_A can choose randomly a point passed through the line and sends chosen point to PBS . It can infer SEED because it knows 2 points to draw linear polynomial. PBS repeat again this process, but point which it will send is generated with PW_2 and T. It searches KS related with P_{id} , and sends KS with randomly determined point. PRS_B receives those, then can extract SEED. MS can be constructed by random function setting SEED. The device of user can overlap MS and KS. Remained pattern is removed except for black because the user can see the medical image blurredly. As the result, the user can view the stacked image as original image.

IV. IMPLEMENTATION

Web-based EHR systems satisfy requirement about remote medical service and more convenient accesses [11]. We develop EHR system founded on “openEMR” referenced to Fig 1. It provides medical practice management application as open source [12]. It is also suitable to fully integrated electronic health records, practice management, scheduling, electronic billing, internationalization, free support, a vibrant community, and a lot more function. It is basically developed by PHP and MySQL.

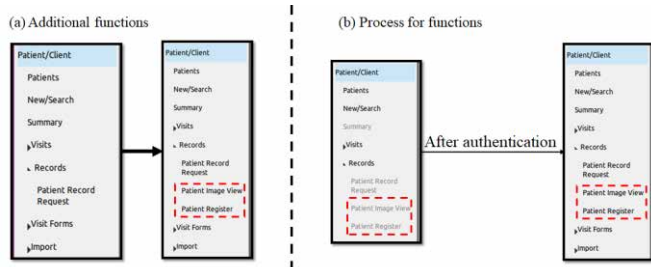


Figure 8. Left bar in openEMR

Two function of proposal mechanism is added to openEMR like (a) in Fig. 8. “Patient Register” function is implemented following to registration process of medical image and “Patient Image View” function is implemented as view process of medical image. If user want to access the functions, user must be authenticated as (b) in Fig. 8.

After authentication of user, “Patient Register” button is activated. First screen of the function seems like left figure of Fig. 9. It shows patient name and id, and includes buttons to select medical image file in device and send the file. If user success for sending the image to *PRS* and *PBS*, user can see the right screen of Fig. 9 In inside system, SEED is saved in affiliated *PRS* and KS is saved in *PBS*.

If another user wants to confirm the medical image with *P_{id}*, user passes through authentication and verifies the image as Fig. 10.

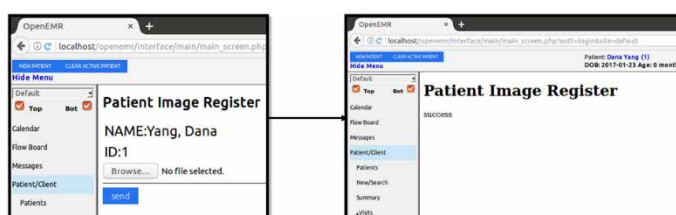


Figure 9. Screen for registration of medical image

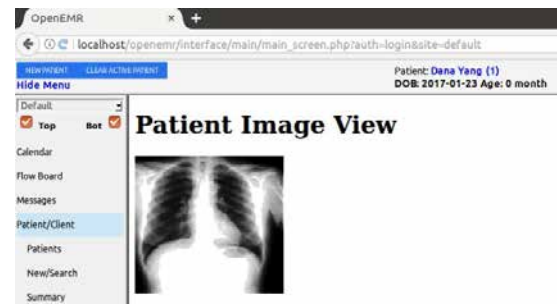


Figure 10. Screen for view of medical image

V. EVALUATION

A. Performance

Our proposal suggests that it is only dependent on share images, because original image is removed. If shared images to be a little different or faulty are stacked, the stacked image will never reveal medical data. Thus, the correlation-based similarity between the original image and the reconstructed image is significantly important [13]. Our mechanism is analyzed using correlation coefficient between each image. The method can identify the degree of relationship between two set of data and be calculated by this formula (1). X means a set value of original image and Y means a set value of stacked image. For accurate calculation, R language is used.

$$\rho_{XY} = \frac{E(XY) - \mu_X \mu_Y}{\sigma_X \sigma_Y} \quad (1)$$

Table 1 presents pictures used for implementation and result of correlation coefficient between related pictures that are “Original Picture” to be previous VC process and “Stacked Picture” to overlap MS and KS after VC process. The result means that the closer 1 becomes, the more similar relation of two set is. Therefore, proposal mechanism has satisfactory performance.

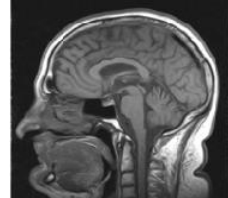
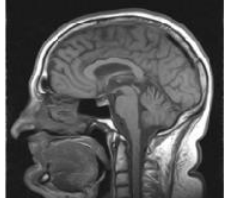
Original Picture	Stacked Picture	Correlation Coefficient
		0.9984009
		1

Figure 11. Total result for evaluation.

B. Security

This mechanism creates diametrically SEED per medical image although one patient takes many EMR pictures. Each participant to share EMR with same SEED generates different polynomial as well as draws different linear lines per time, because one point of linear polynomial involves variable value like current time. In this reason, it is thoroughly impossible that attackers conjecture SEED or polynomial line even though they collect points on communication. However most important fact of all is that they never conjecture EMR image although they invade completely *PRS* or *PBS*, in the reason of VC peculiarity.

This system dose not save the original medical picture and separates shared images. The shared images need to be saved in disjoint systems. In our system, only the KS is saved in *PBS*, and the MS is created and is removed, whenever another *PRS* requests. Although attackers illegally takes the KS in *PBS*, they can never create MS and see the original medical image. Besides, this system can assure more safety from some attacks, because there is no information about MS or KS in *PRS*.

VI. CONCLUSIONS

When sharing information in EHR system dealing with crucial data of patient, significant topics are the method to communicate between the institutions and save EMRs. This paper provides scheme to save data of image type based on VC and share the data by using secrete sharing with password of practitioners. Also it is adapted to practical EHR system using open source "openEMR" by developing proposal function. It is evaluated by correlation coefficient with original picture and reconstructed picture in R language. We can verify superior performance and analyze security. In the future work, we will proceed with sharing data of image type using VC with half-tone and detailed authentication.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP) (No. 2016R1A2B4015899). Kijoon Chae is the corresponding author.

REFERENCES

- [1] Eichelberg, Marco, et al. "A survey and analysis of electronic healthcare record standards." *Acm Computing Surveys (Csur)* 37.4 (2005): 277-315.
- [2] Zhang, Rui, and Ling Liu. "Security models and requirements for healthcare application clouds." *Cloud Computing (CLOUD)*, 2010 IEEE 3rd International Conference on. IEEE, 2010.
- [3] Vincent, Johann, Wei Pan, and Gouenou Coatrieux. "Privacy protection and security in eHealth cloud platform for medical image sharing." *Advanced Technologies for Signal and Image Processing (ATSIP)*, 2016 2nd International Conference on. IEEE, 2016.
- [4] Chen, Qingzhang, Zhehu Wang, and Wangqiao Zhang. "Security Design for Electronic Medical Record Sharing System." *Biomedical Engineering and Computer Science (ICBECS)*, 2010 International Conference on. IEEE, 2010.

- [5] M Naor, A Shamir. "Visual Cryptography." In *Advances in Cryptology – Eurocrypt '94*, Proceedings (Lecture Notes in Computer Science 950) (May 9–12, 1995) A. D. Santis, Ed. Springer-Verlag pp. 1–12.
- [6] Manimurugan, S., and K. Porkumaran. "A new fast and efficient visual cryptography scheme for medical images with forgery detection." *Emerging Trends in Electrical and Computer Technology (ICETECT)*, 2011 International Conference on. IEEE, 2011.
- [7] Yang, Dana, Inshil Doh, and Kijoon Chae. "Enhanced password processing scheme based on visual cryptography and OCR." *Information Networking (ICOIN)*, 2017 International Conference on. IEEE, 2017.
- [8] Shamir, Adi. "How to share a secret." *Communications of the ACM* 22.11 (1979): 612-613.
- [9] Lin, Sian-Jheng, and Wei-Ho Chung. "A Probabilistic Model of $S(t, n)$ Visual Cryptography Scheme With Dynamic Group." *IEEE transactions on information forensics and security* 7.1 (2012): 197-207.
- [10] Gauravaram, Praveen. "Security Analysis of salt| password Hashes." *Advanced Computer Science Applications and Technologies (ACSAT)*, 2012 International Conference on. IEEE, 2012.
- [11] Liu, Qian, et al. "Securing telehealth applications in a Web-based e-health portal." *Availability, Reliability and Security*, 2008. ARES 08. Third International Conference on. IEEE, 2008.
- [12] openEMR Homepage, <http://www.open-emr.org/>, last accessed 2016/6/29
- [13] Studholme, Colin, Derek LG Hill, and David J. Hawkes. "An overlap invariant entropy measure of 3D medical image alignment." *Pattern recognition* 32.1 (1999): 71-86. S. M. Metev and V. P. Veiko, *Laser Assisted Microtechnology*, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

Dana Yang received the B.S. degree in the Department of computer software at Korean BibleUniversity in 2013. She is currently a Ph.D. candidate in the Department of computer science and engineering at Ewha Womans University, Seoul, Korea. Her research interests include visual cryptography, authentication and D2D network security.

Inshil Doh received the B.S. and M.S. degrees in Computer Science at Ewha Womans University, Korea, in 1993 and 1995, respectively, and received the Ph.D. degree in Computer Science and Engineering from Ewha Womans University in 2007. From 1995-1998, she worked in Samsung SDS of Korea to develop a marketing system. She was a research professor of Ewha Womans University in 2009-2010 and of Sungkyunkwan University in 2011. She is currently an assistant professor of Computer Science and Engineering at Ewha Womans University, Seoul. Her research interests include wireless network, sensor network security, and M2M network security.

Kijoon Chae received the B.S. degree in mathematics from Yonsei University in 1982, an M.S. degree in computer science from Syracuse University in 1984, and a Ph.D. degree in electrical and computer engineering from North Carolina State University in 1990. He is currently a professor in Department of Computer Science and Engineering at Ewha Womans University, Seoul, Korea. His research interests are network security including sensor network, smart grid, CDN, SDN and IoT, and network protocol design and performance evaluation.