International Journal of Communication Networks and Security

Volume 1 | Issue 2 Article 8

2011

A Novel approach for Privacy Preserving in Video using Extended Euclidean algorithm Based on Chinese remainder theorem

Anjanadevi B
Department of CSE, MVGR College of Engineering, Vizianagaram, India, banjana3683@gmail.com

P.S.Sitharama Raju
Department of CSE, MVGR College of Engineering, Vizianagaram, India, vicky.poosapati@gmail.com

Jyothi V
Department of CSE, MVGR College of Engineering, Vizianagaram, India, jyothi.vadisala@gmail.com

V.Valli Kumari
Department of CSE, MVGR College of Engineering, Vizianagaram, India, vallikumari@gmail.com

A Novel approach for Privacy Preserving in Video using Extended Euclidean algorithm Based on Chinese remainder theorem

Anjanadevi B[1], P.S.Sitharama Raju[2], Jyothi V[3], V.Valli Kumari[4]
Department of CSE,
MVGR College of Engineering,
Vizianagaram, India
banjana3683@gmail.com[1], vicky.poosapati@gmail.com[2], jyothi.vadisala@gmail.com[3],vallikumari@gmail.com

Abstract – The development in the modern technology paved a path in the utilization of surveillance cameras in streets, offices and other areas but this significantly leads a threat to the privacy of visitors, passengers or employees, leakage of information etc.. To overcome this threat, privacy and security needs to be incorporated in the practical surveillance system. It secures the video information which is resided in various video file types. In this process we used an efficient framework to preserve the privacy while distributing secret among 'N' number of parties. In this paper we analyzed various techniques of Chinese Remainder Theorem.

Keywords - Privacy, secret sharing, CRT, Extended Euclidean algorithm.

I. INTRODUCTION

The Growth of internet has increased the usage and distribution of multimedia content among remote locations. In present internet form is lack of security while distributing the multimedia information. But security of sensitive information [7] is the primary concern in the field of commercial, medical military systems and even at work places.

Information privacy is concerned with preserving the confidentiality of information and is therefore the most relevant kind of privacy with respect to the internet and email monitoring or electronic monitoring [8]. Therefore it vital to develop an efficient method which can ensure that the data is not be tampered. Though encryption techniques are popular and assures the integrity and secrecy of information, single point failure is the major vulnerability [6] for large information (like satellite photos, medical images or even video information) contents.

Thus to resolve those problems secret sharing schemes have been proposed [2][4][5] based on threshold in 1979. Later, the researchers have proposed various techniques based on secret sharing [1][3][15]. But all these techniques have various disadvantages like increase in share size, poor contrast ratio in the reconstructed image or other issues related to security before computation of the image.

Apart from the secret sharing techniques on images, the reviews on video information also clearly focused on the drawbacks of various encryption algorithms viz., DES, AES, etc. which consumes large amount of time for encrypting the video data. Though few algorithms used scrambling technique [17], they were observed to be insecure and even neglected the data format of videos. Still it is found that the size of the video data is drastically increasing which again is an overhead at the time of distribution.

Hence, to overcome these drawbacks, we proposed a new approach using secret sharing technique which is more efficient than the other techniques. In our approach we use Chinese remainder theorem and Extended Euclidean algorithm. The rest of the paper is organized as the Section-I describe how the privacy is preserved before secret distribution. Section-II describes the Privacy preserving using secret sharing and Section-III explains about original results. Section-IV concludes the paper..

II. PRIVACY PRESERVATION

Now a day, privacy is major concern in video transmission. Before transmission of video from one place to another, it is essential to change the form of the information to provide security, to the information to be transmitted. Hence, to attain this process, consider a video file(.avi or .mpg) and split into number of frames. Select one of the frames F from video V. For enabling the distributed secured processing, frame F is distributed to N number of parties. If frame F is directly distributed, there is a chance of information leakage. Hence, to avoid information leakage, we need to maintain privacy to the input frame. In this process, scaling (scale the positive integer with each pixel) and randomization (generation of random number and summation with each pixel) are applied to the frame. After scaling and randomization, the frame is processed for secret sharing.

Secret Sharing

Advantages

1.Before the secret is shared to multiple parties, it is transformed from one type of structure to other so that the structure is preserved.

2. In shamir's secret sharing technique Lagrange interpolation shows that t + 1 participants can recover the polynomial and thus secret s.

3. In our approach the advantage over the Shamir's and other secret sharing schemes is that,here we are maintaining secrecy while distributing the shares and computationally efficient.

disadvantages

1. Traditional use of secret sharing is for small secrets.
2. In Shamir's secret sharing, if we want to share a large secret the share size has impact on computation and communication. To share an m-bit secret amongst n players, we need to distribute nm bits. To recover a secret, we need to retrieve (t+1)m bits.
3. Ramp threshold secret sharing schemes trade security for communication and storage complexity.

Secret sharing is one of the way to distribute secret among N number of parties. Each party will contain one part of secret. The secret may be a video frame or an image. Each and individual part of secret does not reveal any useful information. While combining all parts together we can construct original image. The original image can be obtained only by combining all the parts.

Initial condition

- Choose N number of relatively primes (gcd(I,J)=1 the I and J are relatively prime), Where N is equal to number of shares to distribute a secret.

Procedure to sharing a Secret

- Split the secret into N number of shares
- Each share is sent to individual computational severs. Here, it is possible to calculate shattering (sharing) time to each server.
- By applying above secret sharing technique, no two shares shall give the original secret. By combining all the shares only we can get the original Secret.

Affine Transformation

This process is applied to each computational server and the operation is independent to each and individual computational server. If this process is not applied on each server, then there is a chance of obtaining the partial result. Thus, on each share we apply the affine transformation individually.

Initial conditions

Consider the N number of shattered shares and apply the affine transformation to each individual shares.

Procedure

Now, apply the additive modular operation to get the affine transformation values for Share1. Repeat the same procedure to all the shares. These t_1, t_2 are positive integers and are used for reconstruction process also.

Various approaches in Merging process

Need of CRT

There are certain conditions where the number is unknown. For this unknown number, when is divided by 19, the remainder is 18. When it is divided by 29, the remainder is 4 and when it is divided by 31, the remainder is 23.

i.e $X \equiv 18 \bmod 19$
$X \equiv 4 \bmod 29$
$X \equiv 23 \bmod 31$

To solve this system, we found a unique solution of the system in various ways which are differentiated in time variance.

Algorithm-I

Let $a_1,a_2,a_3,\ldots\ldots\ldots\ldots a_n$ are the arbitrary integers

$P_1,p_2,p_3\ldots\ldots\ldots\ldots\ldots p_n$ are relatively primes i.e Each pair of moduli $GCD(P_i,P_j)=1$ for $i \neq j$

$X \equiv a_1 \bmod p_1$
$X \equiv a_2 \bmod p_2$
$X \equiv a_3 \bmod p_3$
. . .
. . .
. . .

$X \equiv a_n \bmod p_n$

It has exactly one common unique solution.

One way to solve the above system of congruencies, one should choose a positive integer Y i.e $0<Y\leq M$ where $M=p_1*p_2*p_3\ldots\ldots p_n$. Here Y is a unique solution modulo M. If Y is unique then Y modulo p_1,we get a_1 value and Y modulo p_2,we get a_2 value similarly we solve all system of congruencies.

The above one is the simple way to find a unique solution. But here the disadvantage is repeatedly checking of all positive integers from 1 to Y. It takes more time to calculate modular operations to all positive integers from 1 to Y.

Algorithm-II

Proof:

We need to show that a solution exists and that is unique modulo M.

Here we used **Chinese Remainder Theorem (CRT)**

To construct a simultaneous solution,

Let $M_i=M/m_i$

K=1,2,3,……,n.

Where, Mi is the product of moduli except for **ith** term.

In this, $GCD(M/m_i,m_i)=1$.

Using, **Extended Euclidean algorithm**,

We can find N_i such that

$M/m_i*N_i \equiv 1 \bmod mi$

Then $X \equiv a_1*(M/m_1)*N_1+ a_2*(M/m_2)*N_2+ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots+ a_r*(M/m_r)*N_r.$

i.e $X \equiv a_i*\{M/m_i\}*N_i$

Rest of the terms yield the result to a value zero, Since $M/m_j \equiv 0 \bmod m_i$, when $i\neq j$.

X satisfies all the congruencies in the system. X is the unique solution for modulo M.

In this process, consider any video file(eg: .mpeg video), split into number of frames. Choose any input frame and apply scaling & randomization to preserve the privacy. Now, Scaled and Randomized image doesn't reveal any useful information. Hence, using the secret sharing technique, we can achieve the efficient privacy preserving process. Figure 1.c, Figure 1.d and Figure 1.e are the individual shares those are sent to computational servers.

III. EXPERIMENTAL RESULTS

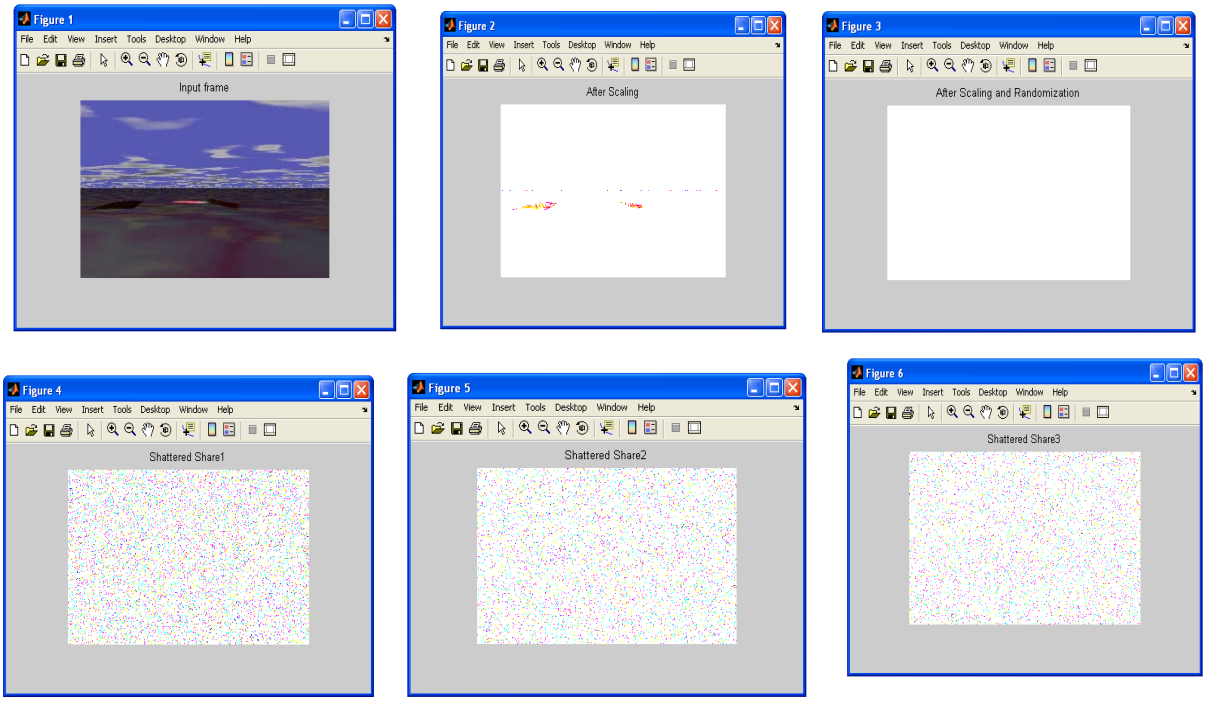

Figure 1.:(a)Input Frame taken from video. (b)Frame After Scaling. (c)After Scaling and Randomization (d) Share1 of the input frame (e)Share2 of the input Frame (f)Share3 of the input frame

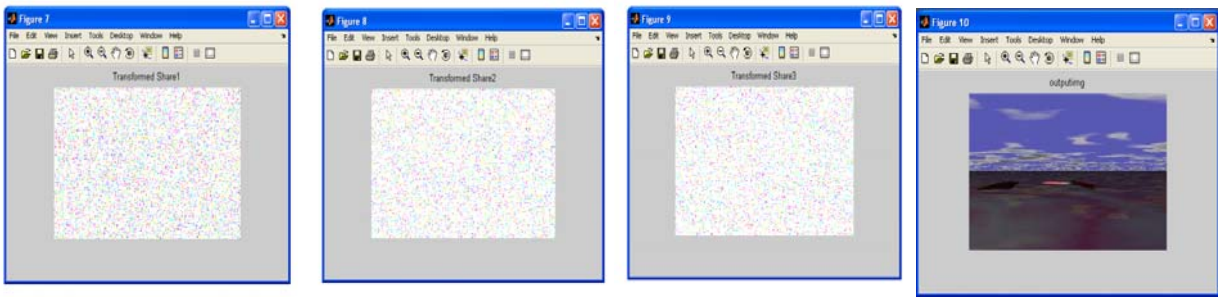

Figure 2: (a) Transformed Share1 (b) Transformed Share2 (c) Transformed Share3

In this approach we used three computational servers to perform the transformation of shares. There we applied transformation which is used in reconstruction phase (for retrieving original image). Here d_i is the pixel values of the shares and SC is the positive scale factor and pi is prime numbers of the corresponding shares. Affine transformation is independent of each computational server. The corresponding Transformed shares are shown in Figure 2. Finally, Observer will merge these three transformed shares using efficient Chinese Remainder Theorem with PSNR (Peak-Signal-Noise-Ratio)value above 53.Our Transformation will gives loss-less result in less time.

The merging algorithm is applied on 3 different types of videos and the PSNR values calculated with various

scaling factors. The table-1 below explains the PSNR values for different scaling factors.

TABLE 1: PEAK SIGNAL – TO – NOISE – RATIO

Image resolution	Scaling Factor		
	33	80	120
DFS.AVI (320 x 240)	56.624	99	99
DELTA.MPEG (320x200)	53.8	99	99
POD.AVI (320 x 240)	55.025	99	99

IV. CONCLUSION

In this approach, we obtained the results in much effective manner and also found that the computational time is less when compared to the other techniques. It is also observed that the size of the output image file is almost equal to the original size where in other techniques; it is found that the output file size is larger than the original one. Hence, our approach is more efficient than others.

REFERENCES

[1] C.C. Asmuth, J. Bloom. "A modular approach to key safeguarding". IEEE Transactions on Information Theory, 1983: Pp.: 208 – 210.

[2] A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612-613,Nov. 1979

[3]. A. Beimel and B. Chor, "Secret sharing with public reconstruction," vol. 44, no. 5, pp. 1887 – 1896, Sept.1998.

[4]. G. Blakley, "Safeguarding cryptographic keys," presented at the Proceedings of the AFIPS 1979 National Computer Conference, vol. 48, Arlington, VA, June 1997, pp. 313 - 317.

[5] T. Migler, K. E. Morrison, and M. Ogle, "Weight and rank of matrices over finite fields," September 29, 2003. Online available at:

http://www.calpoly.edu/kmorriso/Research/weight.pdf.

[6] Li Bai, Saroj Biswas, Albert Oritz and Don Dalessandro, " An Image Secret Sharing Method", IEEE Xplore, 2007.

[7] C.C. Thien and J.C. Lin, "Secret image sharing," Computers & Graphics, vol. 26, no. 5, pp.765 - 770, 2002.

[8]. Hazel Oliner, "Email and internal monitoring in the Workplace: Information Privacy and Contracting out", Industrial Law Journal 321 – 322, (2002) 31 (4).

[9] Maneesh Upmanyu, Anoop M. Namboodiri, Kannan Srinathan and C.V. Jawahar, "Efficient Privacy Preserving Video Surveillance", In Twelfth International Conference on Computer Vision (ICCV), 2009.

[10]. Shai Avidan, Moshe Butman, "Efficient Methods for Privacy Preserving Face Detection", In NIPS, pages 57–64, 2006.

[11]. A. C. Yao. "Protocols for secure computations". In Proc. 23rd IEEE Symp. on Foundations of Comp. Science, pages 160–164, Chicago, 1982. IEEE.

[12]. O. Goldreich. "Foundations of Cryptography: Volume 1, Basic Tools". Cambridge University Press, New York, 2001.

[13]. Bruce Schnier, " Applied Cryptography", John Wiley & Sons, New York.

[14]. C Narasimha Raju, Ganugula Umadevi, Kannam Srinathan and C V Jawahar, "A Novel Video Encryption Technique Based on Secret Sharing", ICIp 2008,

[15]. E. D. Karnin, J. W. Greene, and M. E. Hellman, "On secret sharing systems," vol. IT-29, no. 1, pp. 35-41, Jan. 1983.

[16]. S. Avidan and M. Butman. "Blind vision". In Proc. of European Conference on Computer Vision, 2006.

[17]. L Tang, "Methods for Encrypting and Decrypting MPEG video data Efficiently," in Proc. Of ACM Multimedia,pp.219-229.