Anjanadevi B,Nagesh Vadaparthi, Jyothi V,Satyanarayana Reddy G/ International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 1, January -February 2013, pp.560-566

A Novel Approach For Privacy Preserving Videosharing And Merging

Anjanadevi B,Nagesh Vadaparthi, Jyothi V,Satyanarayana Reddy G
Department of IT, MVGR College of Engineering, Vizianagaram, AP, India

Abstract

In present days rapid growth of internet has paved a path for increased utilization of distributed applications. The number of applications aredrastically increased for a distribution of video information to various places. In recent years, videos are also playingmajor role at various surveillance applications. Hence, propose a novel approach to share the videos to various places while providing privacy.In this paper we used an efficient algorithm to merge the given video. This method provides various parameters to preserve the privacy and accuracy. Our proposed framework is highly efficient than various existing approaches like Smart Cameras, Homomorphic Encryption and Secure Multi-Party computation to carry out privacy preserving video surveillance. This work opens up a new avenue for practical and provably secure implementations of vision algorithms. The proposed system along with motion segmentation results will be used to detect and track peoples or objects.

Index Terms-Privacy, Video Surveillance, Sharing algorithm, Merging Algorithm, Vision algorithms

I. INTRODUCTION

The Growth of internet has increased the usage and distribution of multimedia content among remote locations.In present internet form, lack of security is observed while distributing the multimedia information.But security of sensitive information [1] is of primary concern in the field of commercial,medical, military systems and even at work places.Privacy plays a major role in internet applications. Privacy is pertains to data is "freedom from unauthorized intrusion". With respect to privacy-preserving data mining [2]. If users have given the authorization to use data for the particular data mining task, then there is no privacy issue. And also the user is not authorized, what user constitutes "intrusion" A common standard among most privacy laws (Ex-European Community privacy guidelines or the U.S. healthcare laws) is that privacy only applies to "individually identifiable data". By combining intrusion and individually identifiable leads to a standard to judge privacy preserving data mining. A privacy-preserving data mining technique must ensure that
any information which is disclosed "cannot be traced to an individual" or "does not constitute an intrusion ".

An improvement in our knowledge about an individual could be considered an intrusion. The latter is particularly likely to cause a problem for data mining, as the goal is to improve our knowledge. Even though the target is often groups of individuals, knowing more about a group does increase our knowledge about individuals in the group. This means we need to measure both the knowledge gained and our ability to relate it to a particular individual, and determine if these exceed the thresholds.Privacy, therefore, happens to be serious concern in the age of video surveillance. Widespread usage of surveillance cameras [3], in offices and other business establishments, pose a significant threat to the privacy of the employees and visitors. It raises the specter of an invasive `Big Brother' society. In this regards, certain privacy laws have been introduced to guard an individual's privacy/rights. Despite these, video surveillance remains vulnerable to abuse by unscrupulous operators with criminal or voyeuristic aims and to institutional abuse for **incriminatory** purposes. These legitimate concerns frequently slow the deployment of surveillance systems. The challenge of introducing privacy and security in such a practical surveillance system has been stifled by enormous computational and communication overhead required by the solutions.

The privacy of the system is based on splitting the information present in an image into multiple shares. The parameters used for shattering are primes $p_1,p_2,p_3\ldots\ldots p_i$ and scale factor 'sc' are constant for each shattering operation and are in general assumed to be public. The only possible information leakage of the secret is that retained by each share. We now analytically show that with an optimal parameter selection, the information retained by a share is negligible.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 [3]. Therefore, it is essential to develop an efficient method which can ensure that the data is not tampered. Though encryption techniques are popular and assures the

integrity and secrecy of information, single point failure is the major vulnerability [3] for large information (like satellite photos,medical images or even video information) contents. Privacy in the workplace is a very important issue that can cause some controversy. There are certain privacy laws that are designed to protect employees and when using video surveillance, privacy of employees must be considered [4]. Privacy issues on video surveillance cameras are most likely to occur when the employees do not realize that they are being filmed (covert video surveillance) or when cameras are located in places where people do not want to be filmed. There are also concerns that, video surveillance (particularly covert video surveillance) may unfairly target certain minority groups.

Video surveillance is a critical tool for a variety of tasks such as law enforcement, personal safety, traffic control, resource planning, and security of assets, to name a few. Rapid development/deployment of closed circuit television *(CCTV)* technology plays a key role in observing suspicious behavior. However, the proliferation in the use of cameras for surveillance has introduced severe concerns of privacy. Everyone is constantly being watched on the roads, offices, supermarkets, parking lots, airports, or any other commercial establishment. This raises concerns such as, watching you in your private moments, locating you at a specific place and time or with a person, spying on your everyday activities, or even implicitly controlling some of your actions. Advantage of video surveillance is it keeps track of video information for future use and is helpful in identifying people in the crime scenes etc. Disadvantage of the present system is that it is difficult to maintain heavy amount of raw video data and Human interaction. This requires higher bandwidth for transmitting the visual data.

Privacy preserving video surveillance addresses these contrasting requirements of confidentiality and utility. The objective is to allow the general surveillance to continue, without disrupting the privacy of an individual. This novel technology addresses the critical issue of ―privacy invasionin an efficient and cost-effective way. Privacy concerns often prevent multiple competitive organizations from sharing and integrating data taken from various videos. In traditional approaches, various algorithms are developed to prevent privacy in some extent. But in privacy preserving video surveillance uses the secret sharing technique to achieve complete privacy and efficient computation of surveillance algorithms.

Role of Visual Data

While general purpose secure computation appears to be inherently complex and oftentimes impractical, we show that due to certain "suitable" properties of visual information, efficiency and security co-exists in the domain of computer vision. We exploit the following facts, which are valid for most of the computer vision tasks. Meaningful images from real-world have following properties that are of interest to us.

Limited and fixed Range

The values that an algorithm can take are finite and are from a limited fixed range. And more importantly the range is known aprior [5]. Thus, the algorithms that have multiple possible answers, but only one of them within this possible range, are as valid as solutions that have only one answer. Such algorithms need not be useful (or correct) for a general purpose (non-vision) tasks. In this approach, we have exploited this by designing efficient, secure surveillance solutions that has infinite answers, but only one of them in the valid range. Interestingly, in this process, we I also circumvent Oblivious Transfer, thereby gainingin efficiency.

Scale Invariance

The information in the image remains practically unchanged even if we change the units of measurement or scale the whole data. This is not true for most non-image information. We exploit this to design a wrapper algorithm which converts a partially secure algorithm to a completely secure one. For example, consider a partially secure algorithm that may reveal the LSB of all the pixels. Suppose this algorithm is run on an input which is scaled (at least by a factor of two) with all the LSBs randomized. Then note that with practically no change in the output, the original input (before scaling) is completely secure. Keeping in mind the above properties, this design is a vision specific, distributed framework for surveillance tasks that preserves privacy. The emphasis is on performing this efficiently, thus facilitating proactive surveillance. In this framework, each video is shattered into shares and each one is sent to a different site in such a way that each site has no information about the scene (data-specific secret sharing). The complete algorithm runs in this distributed setup, such that at the end of the protocol, all that the observer recovers is the final output from the results obtained at each of the site.The extent to which employers can use video surveillance to monitor employees may depend on the state they are living in and the type of business they are conducting. In most cases, employees should be notified of the video surveillance that is taking place and the video surveillance should not include areas where employees have a right to expect some privacy. In some cases, covert video surveillance is allowed (for instance, when an employee is suspected of criminal activity), but an employer may need to get permission from the relevant authorities before implementing this. General video surveillance for security purposes

will, in most cases, not be considered to breach any privacy rights in the workplace.Video surveillance is not the only type of monitoring that may be conducted in the workplace.

Thus, to resolve these problems, secret sharing schemes have been proposed based on threshold in 1979. Secret Sharing refers to a method for distributing a secret among a group of servers each of which is allocated a share of the secret [6]. The secret can be reconstructed only when the shares are combined together; on their own, the individual shares give no information of the secret. Several types of secret sharing schemes have been proposed in literature**.** Shamir'**s** secret sharing scheme [6] represents the secret as the y-intercept of an n-degree polynomial, and shares correspond to points on the polynomial. In contrast, Blakley'**s** scheme specifies the secret as a point in n-dimensional space [3], and gives out shares that correspond to hyper planes that intersect the secret point. The primary motivation behind Secret Sharing is of securing a secret over multiple servers. However, computing functions on the input secretly shared among *n*-servers requires highly communication intensive protocols (which relies on some sort of SMC). Furthermore, such schemes result in huge data expansion, which becomes in-efficient for large secrets, such as live-videos (as in our case). For example, Shamir's shares are each as large as the original secret, where as Blakley's scheme is even less space-efficient than Shamir's. Each secret share is a plane, and the secret is the point at which three shares intersect. Two shares yield only a line intersection.

The primary motivation is proposing a paradigm shift for our real-timetasks was to reduce communication. We next show that visual-data has certain characteristic properties, which can be exploited to define a tailor made Secret Sharing scheme exclusively for visual data. Compared to the standard CRT based Secret Sharing schemes, our scheme significantly reduces the data expansion by at least a factor of,where is the number of servers/shares. Such reduction is prominent for huge data such as live-video feeds, thus making privacy preserving video surveillance practical.

Video surveillance techniques Public Key Encryption (PKC)

The process of converting the plaintext (P) to cipher text (C) using an algorithm is called encryption (E). On the other hand, restoring the plaintext from the cipher text is called decryption (D). Public key Encryption (PKC), also known as asymmetric cryptography, is a form of cryptography in which key used to encrypt a message differs from the key used to decrypt it. Private Key is kept secret, while the public key can be widely distributed. The message that needs to be conveyed to the recipient is encrypted using his public key. It can only be decrypted by the corresponding private key. These keys are related mathematically, but the private key cannot be practically derived from the public key.

In practice, PKC can be used to ensure confidentiality of the data. The messages encrypted with a recipient‘s public key can only be decrypted using the corresponding private key. The private key of which is known only to the intended receiver. Asymmetric key algorithms are generally found to be computationally expensive. Some ofthe popular PKC algorithms include Pailliers and El-Gamal.

Secure Multi-Party Computation(SMC)

In cryptography, secure multi-party computation or secure computation or multi-party computation (MPC) is a problem that was initially suggested by Andrew C. Yao [5] in 1982 paper. In that publication, the millionaire problem was introduced: Alice and Bob two millionaires who want to find out who is richer without revealing the precise amount of their wealth. Yao proposed a solution allowing Alice and Bob to satisfy their curiosity while respecting the constraints. The concept is important in the field of cryptography and is closely related to the idea of zero-knowledgeness.

In general, it refers to computational systems in which multiple parties wish to jointly compute some value based on individually held secret bits of information, but do not wish to reveal their secrets to one another in the process. For example, two individuals who each possess some secret information—*x* and *y*, respectively—may wish to jointly compute some function f(x,y) without revealing any information about *x* and *y* other than can be reasonably deduced by knowing the actual value of f(x,y), where "reasonably deduced" is often interpreted as equivalent to computation within polynomial time.

The primary motivation for studying methods of secure computation is to design systems that allow for maximum utility of information without compromising user privacy. SMC uses interactions between multiple parties to achieve a specific task, while keeping everyone oblivious of others data. Introducing privacy and security in visual data processing was attempted with considerable success in different domains. Blind vision [7] allows someone to run their classifier on another person‘s data without revealing the algorithm or gaining knowledge of the data. Shashank exploited the clustered nature of image databases to improve the efficiency of SMC for example based image retrieval by processing multiple queries together.

Smart Cameras

Smart cameras do surveillance in the camera itself or try to mask sensitive information in the videos. The former requires expensive programmable cameras and are restricted to single

camera algorithms. Changing the algorithms is tedious and costly. The second approach addresses problem specific concerns in surveillance videos. Face swapping and face de-identification [8] try to modify face images such that they can be automatically detected, but cannot be correctly recognized. Face detection techniques uses programmable cameras to carry out detection and masking of the regions of interest.

All the above approaches rely on the success of detection of interest regions and do not provide any guarantee of privacy. Moreover, the original video is lost in all. We note that most of the current privacy preserving algorithms are based on the generic framework of SMC requires heavy communication to achieve secure computation. For instance, a single multiplication is carried out via complex distributed protocol involving oblivious transfer [9], which is a highly communication intensive subroutine in SMC.

Factually, the round-trip time in a LAN is of the order of a few milliseconds, whereas several floating operations take no more than few nanoseconds. Clearly, these delays are too high, while dealing with voluminous data like surveillance videos. Hence, solutions based on SMC are impractical for our application. In this work, the paradigm of secret sharing is to achieve private and efficient computation of surveillance algorithms [10]. Secret sharing (SS) methods [11,12] try to split any data into multiple shares such that no share by itself has any useful information, but together, they retain all the information of the original data. However, the standard SS methods, which were invented to address secure storage of data, results in significant data expansion (each share is at least the size of the data).

Computing on the shares is inefficient as it would require some sort of SMC. In this work, we exploit certain desirable properties of visual data such as fixed range and insensitivity to data scale, to achieve distributed efficient and secure computation of surveillance algorithms in the above framework. This approach also addresses the concerns related to video surveillance, presented below. To achieve distributed secure processing and storage and also address these issues more effectively we have developed a new system to supporting privacy preserving video surveillance.

But all these techniques have various disadvantages such as increase in share size,poor contrast ratio in the reconstructed image or other issues related to security before computation of the image.

Hence, to overcome these drawbacks, a new approach is proposed using sharing and Merging algorithms, which are more efficient than the other techniques. In this approach, we have utilized Chinese remainder theorem for merging various shares into a secret. The rest of the paper is organized as follows, Section-I describes the procedure to preserve the privacy before secret distribution andSection-II explains the Privacy preserving technique using sharing algorithm and Merging algorithm section-III describesthe ExperimentalResults and finally, Section-IV concludes the paper.

Privacy is a 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 which is to be transmitted. Therefore, 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.

II. PRIVACYPRESERVINGTECHNIQUE USING SHARING ALGORITHM AND MERGING ALGORITHM

Input: Capturing a video from camera and spilt into frames.

Step1: Initially, choose N number of relatively primes(gcd(I,J)=1 the I and J are relatively prime) where N equal to number of shares.

Step2: Apply the Scaling (Scale the pixels with fixed integer i.e.,sc) and Randomization (adding randomvalues to each pixel) for ensuring accuracy before sharing algorithm.

To obtain the shares from the secret S as

share1= S mod p_1,
share2= S mod p_2,
share3=S mod p_3

shareN=S mod p_N,
where, $P_1, P_2, \ldots . P_N arerelativelyprime.$

Step3: Each share is sent to individual computational severs and apply the affine transformation on each individual computational server.

Step4: Affine Transformation on share1 as $(p.d_i + q.scmodp1$, where p,q are fixed values which are used for privacy and d_i is pixel values of share1 and sc is scaling factor.

Step5: Affine Transformation is applied to each independent server and keeps results for obtaining original result.

MERGING ALGORITHM

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

1. To construct a simultaneous solution, Let $M_i = M / m_i, i=1,2,3,\ldots\ldots\ldots\ldots\ldots,n$. Where, M_i is the product of moduli except for i^{th}term.
2. In this, GCD($M/m_i, m_i$)=1. Using Extended Euclidean algorithm
3. We can find N_i such that $M/m_i * N_i \equiv 1 \bmod m_i$ Then,
4. $X \equiv a_1*(M/m_1)*N_1 + a_2*(M/m_2)*N_2 + \ldots\ldots\ldots + a_r*(M/m_r)*Nr.$
5. Therefore, $X \equiv a_i*\{M/m_i\}*N_i$

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.

Using Merging Algorithm to solve

$X \equiv 2 \bmod 3,$

$X \equiv 3 \bmod 5,$

$X \equiv 4 \bmod 11,$

$X \equiv 5 \bmod 16.$

Clearly, the moduli are relatively prime in pairs.

$M = 3*5*11*16 = 2640.$

$M_1 = 2640/3 = 880, M_2 = 2640/5 = 528, M_3 = 2640/11 = 240, M_4 = 2640/16 = 165.$

We have

$880*N_1 \equiv 1 \bmod 3,$

$520*N_2 \equiv 1 \bmod 5,$

$240*N_3 \equiv 1 \bmod 11,$

$165*N_4 \equiv 1 \bmod 16.$

Solving using the Extended Euclidean algorithm, we have $N_1 = 1$, $N_2 = 2$, $N_3 = 5$, $N_4 = -3$.

Therefore, $x = 2*880*N_1 + 3*528*N_2 + 4*240*N_3 + 5*165*N_4$

$= 2*880*1 + 3*528*2 + 4*240*5 + 5*165*(-3)$

$= 7253 \pmod{2640}$

$= 1973.$

We have $x = 1973$ as a common solution to the above system of congruence. All other solutions are of the form $1973 + M*i, i=1, 2, 3 \ldots$ and so on.

III. EXPERIMENTAL RESULTS

In this process, consider any video file(eg: walk.avi), 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 which are sent to the computational servers.

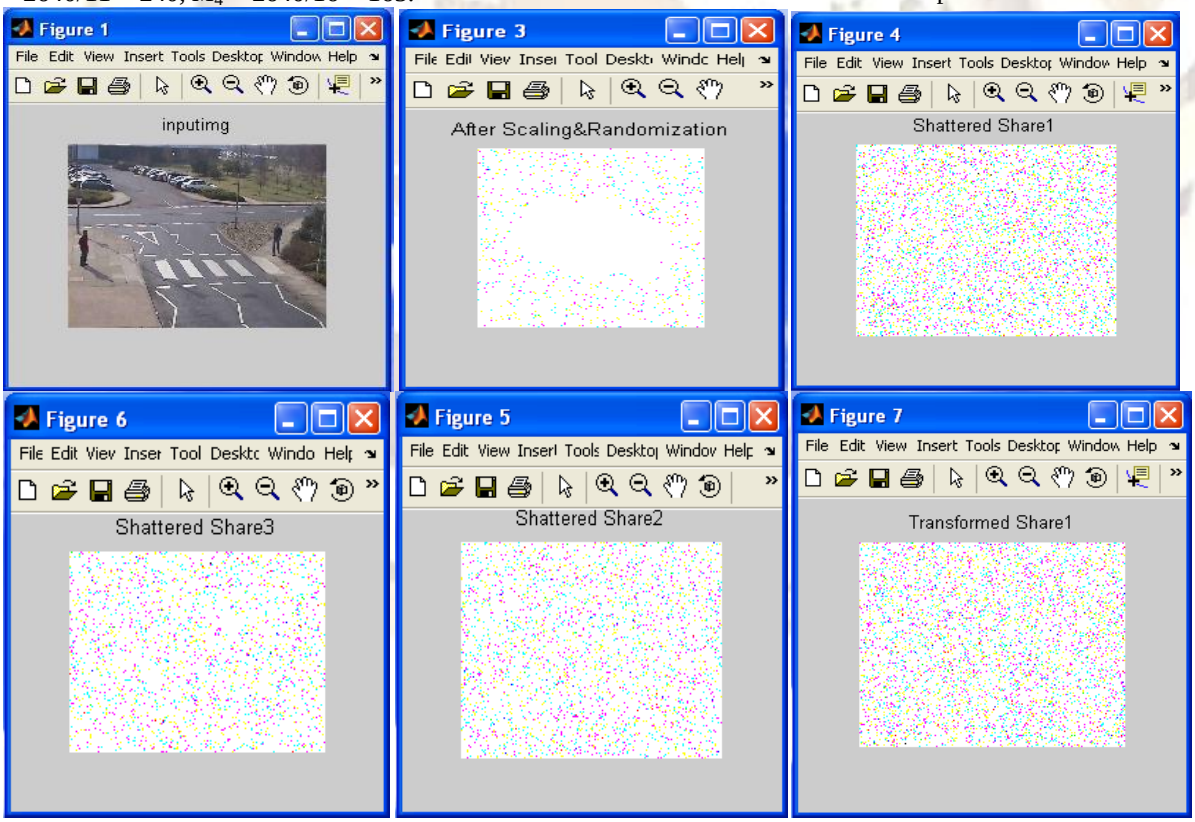


Figure 1.:(a)Input Frame taken from video. (b) After Scaling and Randomization (c)Share1 of the input frame (d)Share2 of the input frame (e)Share3 of the input Frame (f)Transformed Share1 of the input frame

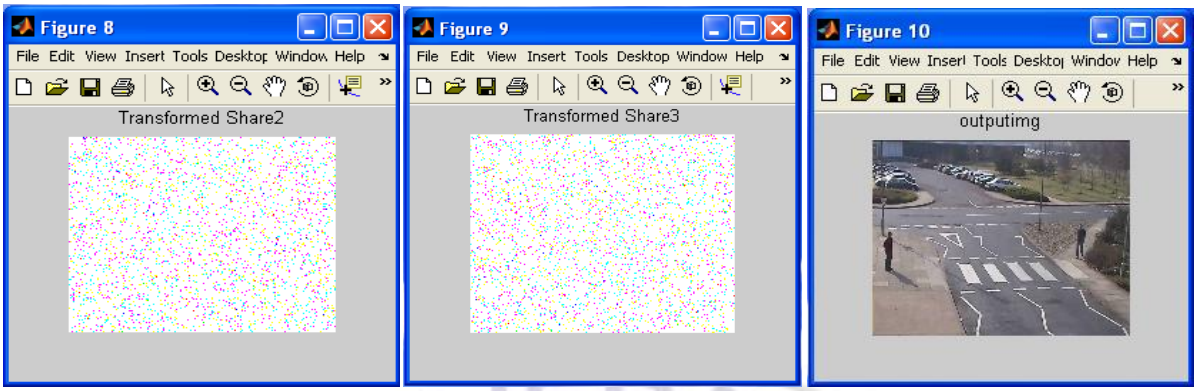


Figure 2: (a)Transformed Share2 (b)Transformed Share3 (c) Reconstructed Frame

In this example, we used three computational servers to perform the transformation of shares. There, we applied transformation formula ($p.d_i+q.SC$) mod p_i, here p,q are positive integers that are 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 p_i is the prime number 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 sharing and merging algorithms.Our Transformation will give loss-less result in less time.

In this section, we also presented few other experimental results where sharing and Merging algorithms applied.

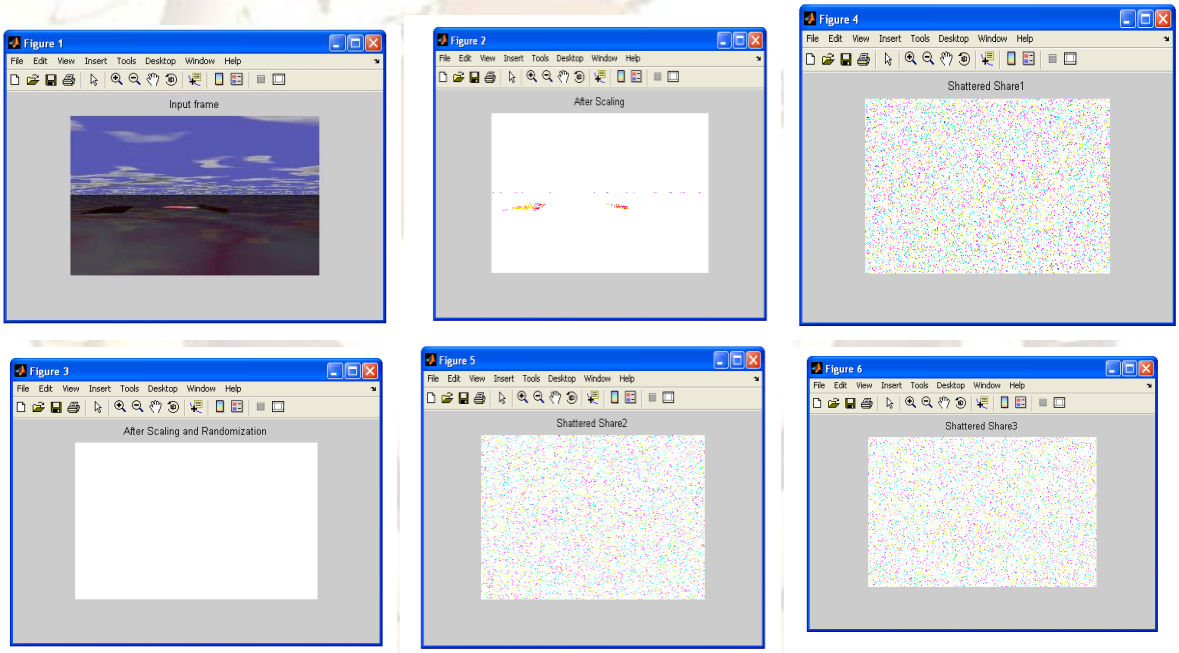


Figure 3.:(a)Input Frame taken from video. (b)Frame After Scaling.(c)After Scaling and Randomization (d)Share1 of the input frame (e)Share2 of the input Frame (f)Share3 of the input frame

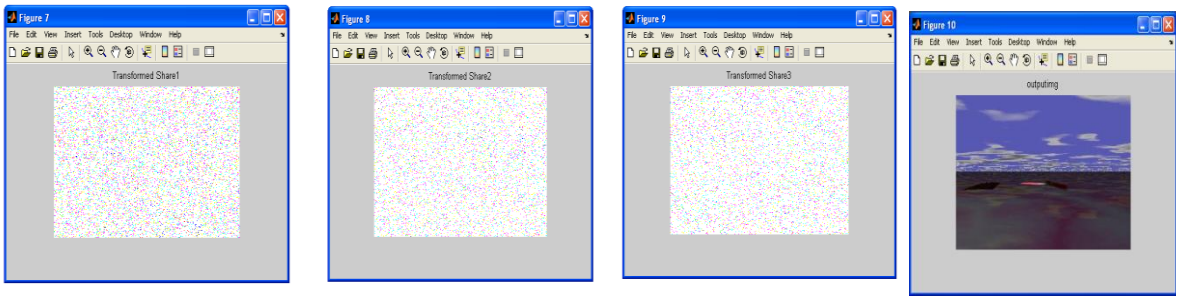
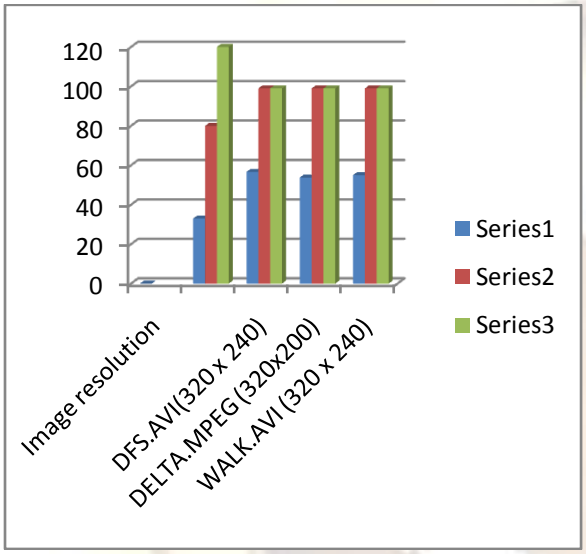


Figure 4: (a)Transformed Share1 (b)Transformed Share2 (c)Transformed Share3(d) Reconstructed Frame

The merging algorithm is applied on 3different types of videos and the PSNR values are calculated with various scaling factors. The table-1 below shows 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
WALK.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.This approach opens up a new avenue for practical and provably secure implementations of various vision algorithms where distribution of data is over multiple computers. These results as guidelines along with motion segmentation can detect and track peoples.

REFERENCES

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

[2] An Introduction to Privacy-Preserving Data Mining *Charu C. Aggarwal, Philip S. Yu. Online available at* http://www.charuaggarwal.net/toc.pdf.

[3] ManeeshUpmanyu, Anoop M. Namboodiri, KannanSrinathan and C.V. Jawahar, “Efficient Privacy Preserving Video Surveillance”, In *Twelfth International Conference on Computer Vision (ICCV)*, 2009.

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

[5] A. C. Yao. “Protocols for secure computations”.InProc. 23rd IEEE Symp.on Foundations of Comp. Science, pages 160–164, Chicago, 1982. IEEE.

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

[7] S. Avidan and M. Butman. “Blind vision”. In*Proc. of European Conference on Computer Vision*, 2006.

[8] Model-based Face de-idenfication technique is online available at ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1640608

[9] C Narasimha Raju, GanugulaUmadevi, KannamSrinathan and C V Jawahar, “A Novel Video Encryption Technique Based on Secret Sharing”, ICIP 2008.

[10] B.*Anjanadevi, P Sitharama raj,V Jyothi,V,Valli Kumari.* A Novel approach for Privacy Preserving in Video using Extended Euclidean algorithm Based on Chinese remainder theorem**.** *International Journal Communication & Network Security (IJCNS), Volume-I, Issue-II, 2011.*

[11] J. C. Benaloh. Secret sharing homomorphisms: keeping shares of a secret secret. CRYPTO, 283:251–260, 1986.

[12] Craig Gentry. Fully homomorphic encryption using ideal lattices. *STOC*, pages 169–178, 2009.