An Effective Secret Sharing Scheme for N out of N Scheme Using Modified Visual Cryptography

A. Sreekumar[1] and S.Babusundar[2]

Abstract

Secret sharing is concerned with the problem of how to distribute a secret among a group of n participating individuals, or entities, so that only pre-designated collections of individuals are able to recreate the secret by collectively combining their shares of secret. Sharing schemes are useful in military and civilian applications. In the traditional Secret Sharing Schemes, a shared secret information cannot be revealed without any cryptographic computations. Various Secret Sharing Schemes have been proposed. However, the size of the shares and implementation complexity in theses schemes depend on the number of participants. In other words, when a great number of participants are involved, the scheme will become impractical. A secret sharing scheme is called ecient if the total length of the n shares is polynomial in n: In the traditional Visual Secret Sharing Schemes, a shared secret information can be revealed without any cryptographic computations. In this paper we propose an n out of n uniform secret sharing scheme based on visual cryptography. This scheme provides an ecient way to hide a secret information in dierent shares. Further more, the size of the shares is just 1 bit more than the size of the secret, and so it does not vary when the number of participants differs.

[1 & 2] Department of Computer Applications, Cochin University of Science and Technology, Thrikkakara, Kochi - 22. Email : sreekumar@cusat.ac.in, drsbsundar@gmailcom

1. Introduction

Secret sharing scheme is a method of sharing a secret information among a group of participants. In a secret sharing scheme, each participant gets apiece of secret information, called a share. When the allowed coalitions of participants pool their shares, they can recover the shared secret; on the other hand, any other subsets, namely non-allowed coalitions, cannot recover the secret information by pooling their shares. The collection of subsets of participants that can reconstruct the secret in this way is called access structure. Secret Sharing was introduced by Blakley [8] and Shamir [1] in 1979. Shamir's solution is based on the property of polynomial interpolation in nite elds; Blakley formulated and solved the problem in terms of nite geometries. The rst secret sharing schemes considered were threshold schemes. A *(k, n)* threshold scheme allows a secret to be shared among n participants in such a way that any k of them can recover the secret, but any *k-1*, or fewer, have absolutely no information on the secret.

Asmuth and Bloom [2] implemented *a (k, n)* threshold scheme based on Chinese Remainder Theorem in 1983.

In [25]D. R. Stinson and S. A. Vanstone introduced anonymous threshold scheme. Informally, in an anonymous secret sharing scheme the secret is reconstructed without the knowledge of which participants hold which shares. In such schemes the computation of the secret can be carried out by giving the shares to a black box that does not know the identities of the participants holding those shares. During 1987 Ito,

Saito, and Nishizeki [16] described a generalized method of secret sharing scheme whereby a secret can be divided among a set P of trustees such that any qualied subset of P can reconstruct the secret and unqualied subsets cannot. Phillips and Phillips [22]considered a dierent model for anonymous secret sharing schemes. In their model, dierent participants are allowed to receive the same shares. Further results on this type of anonymous secret sharing schemes can be found in [10].

Redistributing secret shares to new access structures has been considered in [9]. Secret Sharing schemes based on Chinese Remainder Theorem is introduced by Mignotte [20]. D. R. Stinson[26] gives a comprehensive introduction to this topic.

A black-box secret sharing scheme for the threshold access structure is one which works over any nite Abelian group. G. Bertilsson and Ingemarsson [7] describes a construction method of practical secret sharing schemes using Linear Block Codes.

A more general approach has been considered by Karnin, Greene and Hellman [17] who invented the analysis (limited to threshold scheme) of secret sharing schemes when arbitrary probability distributions are involved.

Some other general techniques handling arbitrary access structures are given by Simmons, Jackson, and Martin [19] [24] and also by suggested by Kothari [18].

In [11] Brickell introduced the vector space construction which provides secret sharing schemes for a wide family of access structures. In [26] Stinson proved that threshold schemes are vector space access structures. Various Secret sharing schemes were proposed, but most of them need a lot of computations to decode the shared secret information. While in threshold schemes proposed by Blakley [8] and Shamir [23] and in the vector space schemes given by Brickell [11] the shares have the same size as the secret, in the schemes constructed by M. Ito, A. Saito, and T. Nishizeki [16] for general access structures the shares are, in general, much larger than the secret.

Subsequently, Benaloh and Leichter [6] gave a simpler and more ecient way to realize such schemes. They also proved that no threshold scheme is sucient to realize secret sharing on general monotone access structures. In support of their claim, they have shown that there is no threshold scheme such that the access structure $((A \vee B) \wedge (C \vee D))$ can be achieved.

In [5] Benaloh describes a homomorphism property that is present in many threshold schemes which allows shares of multiple secrets to be combined to form "composite shares" which are shares of a composition of the secrets. An important issue in the implementation of secret sharing schemes is the size of shares, since the security of a system degrades as the amount of the information that must be kept secret increases. If one requires that non-qualied set of participants should have no information on the secret, then the size of the shares cannot be less than the size of the secret. This fact is established by E. D. Karnin, J. W. Greene and M. E. Hellman [17]. In [6] J. C. Benaloh and J. Leichter, proved that there exists an access structure (namely the path of length three) for which any secret sharing scheme must give to some participant a share which is from a domain larger than that of the secret.

Capocelli, De Santis, Gargano and Vaccaro [12] proved that there exist access structures for which the best achievable information rate (i.e., the ratio between the size of the secret and that of the largest share) is bounded away from 1.

Tompa and Woll [27] considered the issue of cheaters in 1988 and could able to detect cheaters. A cheater might

tamper with the content of a share and make the share unusable for combining to retrieve the secret.

The problem of identifying the cheater is solved by the authors. In a sense, it is an improvement on the works of Shamir [23]. In 1994, Naor and Shamir [21] invented a new type of Secret sharing scheme called visual cryptography scheme. It could decode the secret (printed text, hand written notes, pictures, etc.) directly without performing any computation, and the decoder of this scheme was the human visual system. For example, in a *(k, n)* visual cryptographic scheme, a dealer encodes a secret into n shares and gives each participant a share, where each share is a transparency. The secret is visible if k (or more) of participants stack their transparencies together, but none can see the shared secret if fewer than k transparencies are stacked together.

Until the year 1997, although the transparencies could be stacked to recover the secret image without any computation, the revealed secret images (as in [3] [4] [14] [21]) were all black and white. In [28], Verheul and Van Tilborg used the concept of arcs to construct a colored visual cryptography scheme, where users could share colored secret images. The key concept for a c-colorful visual cryptography scheme is to transform one pixel to b sub pixels, and each sub-pixel is divided into c color regions. In each subpixel, there is exactly one color region colored, and all the other color regions are black. The color of one pixel depends on the interrelations between the stacked sub-pixels. For example, if we want to encrypt a pixel of color c_j, we color region i with color c_i on all sub-pixels. If all sub-pixels are colored in the same way, we sees color c_j, when looking at this pixel; otherwise one sees black.

A major disadvantage of this scheme is that the number of colors and the number of sub-pixels determine the resolution of the revealed secret image. If the number of colors is large, coloring the sub-pixels will become a very dicult task, even though we can use a special image editing package to color these sub-pixels. How to stack these transparencies correctly and precisely by human beings is also a dicult problem. Another problem is that when the number of sub-pixels is b, the loss in resolution from the original secret image to the revealed image becomes b.

In [15], Hwang proposed a new visual cryptography scheme which improved the visual effect of the shares (the shares in their scheme were significant images, while those in the previous scheme were meaningless images). Hwang's scheme is very useful when we need to manage a lot of transparencies; nevertheless, it can only be used in black and white images. For this reason, Chang, Tsai and Chen proposed a new secret color image sharing scheme [13] based on modied visual cryptography.

A major disadvantage of this scheme is that the size of the share is in proportion with the number of participants, i.e., the more the participants, the larger the share will become. The ratio of the size of one share to the size of the secret is called the information rate.

2. Peculiarity of Even Parity Strings

Any information can be encoded as a binary string. So it is sucient to consider only binary strings in any secret sharing schemes. The proposed scheme is based on the following theorem :

Theorem 2.0.1 Let T be an even parity binary string of length t. Then we can nd two *POB- Numbers* A and B, both $\in$ POB(t, $\lfloor \frac{t}{2} \rfloor$) such that $T = A \oplus B$.

Proof : We can assume, without loss of generality that, the leading 2m, ($0 \leq m \leq \lfloor \frac{t}{2} \rfloor$) digits of T are 1s and remaining $t - 2m$ (≥ 0) digits are 0s. Now, let $A = PQ$ be the binary string obtained by concatenating the strings P

and Q, where $\overline{P}$ is the string having exactly m 1s, followed by m 0s, and Q is the string having exactly $\lfloor \frac{t-2m}{2} \rfloor$ 1s and $\lfloor \frac{t-2m}{2} \rfloor$ 0s. Then the choice $B = \overline{P}Q$, where, P is the Boolean complement of P, will prove the theorem. However, such a decomposition, in general, need not be unique. We can see that both A and $B \in$ POB (t, $\lfloor \frac{t}{2} \rfloor$) number system. Also, once we find A, we can get B atones, B = T $\oplus$ A. It may be noted that, among the 2m 1s in T, exactly m 1s are in matched position with P, and the other m 1s are in matched position with Q. The bits in P and Q, corresponding to a 0 in T are same (either both 0 or both 1), they are assigned randomly, with ensuring the only condition that, they $\in$ POB (t,$\lfloor \frac{t}{2} \rfloor$).

2.1. The Proposed Secret Sharing Scheme

In this section, we present our method to construct an n out of n secret sharing scheme based on the modied visual cryptography. Assume that the secret can be represented as a binary string $b_1b_2b_3$ .... b_t. Our scheme will generate n shares after attaching a single bit, b_t+1 at the end of the secret. The resulting structure of the share can be described as an n x (t+1) Boolean matrix S = [S_{ij}], where $1 \le i \le n$; $1 \le j \le (t + 1)$. The original secret will be revealed by performing the "XOR" operation (denoted by $\oplus$ and read as ring sum) on each row in S, and deleting the last bit attached at the end. For an n out of n secret sharing scheme, the construction can be described by any Boolean string C. The construction is considered valid if, for any Boolean string S in C, the ring sum, $\oplus$, of each row in S satises the following equation:

$$b_j = S_{1j} \oplus S_{2j} \oplus S_{3j} \oplus .... \oplus S_{nj},$$

for $j = 1, 2, ..., t.$ (1)

Here we dene S is a uniform construction, if, each row of S is a uniform code.

2.2. A Uniform 2 Out of 2 Construction

We now describe the construction details of a uniform 2 out of 2 secret sharing scheme and extend it to a uniform n out of n scheme in the next section. Let $B = b_1b_2b_3...b_t$ be the secret information to be shared between two participants. We describe an ecient (2, 2) scheme by making use of the theorem 2.0.1. First of all, the necessary condition to use the theorem is that, the concerned string must be even parity. So, we extend the secret by appending a single bit at the right end. If we discard the appended last bit, we get precisely the secret. The length of the extended string is just one more than that of the secret. The Algorithm 1 extends the string and makes the resulting string an even parity.

Now, using construction method in theorem 2.0.1, we split this extended string and obtain the two shares. The very simple algorithm 2 nds the decomposition of the extended string, as in theorem 2.0.1. The algorithm 3 shares any binary string between two shares, by using algorithm 1 and then algorithm 2.

Recovery : From $E_{t+1} = S_{t+1}^{(1)} \oplus S_{t+1}^{(2)}$, it follows, if we just discard last bit of E_{t+1} we get B_t. i.e, the recovery procedure is that, just $\oplus$ the two shares, we get the extended string, and discard the last appended bit we get the secret. hence the following lemma :

Lemma 1 The Algorithm 3 described below a (2,2)-modified visual cryptography scheme, in which the size of the secret is just one bit more than the size of secret. More over, all the shares are $POB(t+1, \lfloor \frac{t+1}{2} \rfloor)$-numbers.

The two shares are constructed by using the Algorithm 3 described below :

Algorithm 1 [Append a single bit at the end] Input : A binary string $B_t = b_1b_2 ... b_t$ of length t.

Output : An even parity string $E_{t+1} = e_1e_2 \dots e_{t+1}$ *of length* $t+1$, *such that* $e_i = b_i$, *for* $i \leq t$.

Step 1. $noOfOne = 0$;
For $i = 1$ *to* t *do*
$e_i = bi$;
if $(b_i = 1)$ $noOfOne = noOfOne + 1$;
Step 2. if ($noOfOne$ *is odd*) $e_{t+1} = 1$;
else $e_{t+1} = 0$;
Step 3. The extended string is $E_{t+1} = e_1e_2 \dots e_{t+1}$.

Algorithm 2 *[Sharing an even parity binary string between two blocks]*
Input: An even parity binary string $E_{t+1} = e_1e_2 \dots e_{t+1}$.
Output : Two blocks $S^{(1)}_{t+1} = s^{(1)}_1 s^{(1)}_2 \dots s^{(1)}_{t+1}$ *and* $S^{(2)}_{t+1} = s^{(2)}_1 s^{(2)}_2 \dots s^{(2)}_{t+1}$ *of length* $t+1$ *each.*

Step 1. Set all bits of $S^{(1)}_{t+1}$ *and* $S^{(2)}_{t+1}$ *null.*
Step 2. $noOfOne = 0$;
For $i = 1$ *to* $(t+1)$ *do*
if $(e_i = 1)$ *then*
$noOfOne = noOfOne + 1$;
if ($noOfOne$ *is odd)* $s^{(1)}_i = 1$;
else $s^{(1)}_i = 0$;
Step 3. Randomly assign the rest null bits of $S^{(1)}_{t+1}$ *to 0 or 1,such that* $S^{(1)}_{t+1} \in POB(t+1, \lfloor \frac{t+1}{2} \rfloor)$ *no.*
Step 4. For $i = 1$ *to* $t+1$ *do*
$s^{(2)}_i = s^{(1)}_i \oplus e_i$.

Algorithm 3 *[Sharing any binary string between two blocks]*
Input: A binary string $B_t = b_1b_2 \dots b_t$.
Output : Two blocks $S^{(1)}_{t+1}$ *and* $S^{(2)}_{t+1}$ *each of length* $t+1$

Step 1. Let $E_{t+1} = e_1e_2 \dots e_{t+1}$ *be the extended string obtained Algorithm 1 with the input* B_t.
Step 2. Obtain the shares $S^{(1)}_{t+1}$ *and* $S^{(2)}_{t+1}$ *by Algorithm 2 with input* E_{t+1}.

Algorithm 4 *[Recover the secret information]*
Input : Two shares S_1 *and* S_2 *of 0s and 1s of length* $t+1$
Output: The secret information $B_t = b_1b_2 \dots b_t$.

Step 1. $B_{t+1} = S_1 \oplus S_2$
Step 2. The recovered secret is $B = b_1b_2b_3 \dots b_t$ *(Note that* b_{t+1} *is unwanted.)*

Example 1 :

Let the secret B be

10011 00101 00011 10010 00101 10100

(which corresponds to the word "secret"). Here length of the secret t = 6 * 5 = 30. By Step 1. of Algorithm 3, the extended secret is

B_{t+1} = 10011 00101 00011 10010 00101 10100 1.

By Step 1. of Algorithm 2, Initialize S_1 and S_2 null.

Step 2. of algorithm 2, S_1 is computed as

1 * * 01 * * 0 * 1 * * * 010 * * 1 * * * 0 * 10 * 1 * * 0

(Here * null bits.) Step 3. of Algorithm 2, S_1 is randomly set as

11101100010100100111010010011 10

Step 4. of Algorithm 2, $S_2 = S_1 \oplus B_{t+1}$ =

01110101000101010101100100111

Recovery : Compute S1 ⊕ S2 and get

Bt = 10011001010001110010001011010 01

Last bit is 1 and is deleted to get B : 10011 00101 00011 10010 00101 10100.

2.3. A Uniform n Out of n Construction

Algorithm 5 : [Sharing a secret among n blocks]

Input : A binary string $B_t = b_1b_2 \dots b_t$ *of length t.*

Output : n blocks $S_1, S_2, \dots, S_n$ *of length t + 1.*

Step 1. $b_{t+1} = 0$;
Step 2. Randomly assign n-2 blocks, $\{S_2, \dots, S_{(n-1)}\}$, *with* $\lceil \frac{t+1}{2} \rceil$ *0s and* $\lfloor \frac{t+1}{2} \rfloor$ *1s.*
Step 3. Compute $K_{t+1} = B_{t+1} \oplus S_2 \oplus \dots \oplus S_{(n-1)}$.
Step 4. if (K_{t+1} *is odd parity) then*
$k_{t+1} = \overline{k_{t+1}}$.
$b_{t+1} = \overline{b_{t+1}}$.
Step 5. Compute S_1 *and* S_n *by Algorithm 2, with input* K_{t+1}, *such that,* $K_{t+1} = S_1 \oplus S_n$.

Algorithm 6 : [Recover the secret information]

Input : n shares $S_1, S_2, \dots, S_n$ *of length t + 1*

Output : The secret information $B_t = b_1b_2 \dots b_t$

Step 1. Compute the string $B_{t+1} = b_1b_2b_3 \dots b_{t+1}$ *such that* $B_{t+1} = S_1 \oplus S_2 \oplus S_3 \oplus \dots \oplus S_n$
Step 2. Discard the last bit of B_{t+1} *and the recovered secret* B_t *is* $b_1b_2b_3 \dots b_t$

Lemma 2 The Algorithm 5 described above, is an (n,n)-modified visual cryptography scheme, in which the size of the secret is just one bit more than the size of secret. More over, all the shares are $POB(t+1, \lfloor \frac{t+1}{2} \rfloor)$-numbers.

Proof : It is clear that Step 1 of algorithm 5 appends a single bit at the end of the input string B_t and obtain an

extended string B_{t+1}. Note that the last bit appended is insignicant. In Step 2. it generate *n-2* shares, $S_2, S_3, \ldots, S_{n-1}$. They are all random *POB* (t+1, $\lfloor \frac{t+1}{2} \rfloor$) numbers. In Step 3, from the equation,

$$K_{t+1} = B_{t+1} \oplus S_2 \oplus \ldots \oplus S_{(n-1)} \quad (2)$$

the following equation holds :

$$B_{t+1} = K_{t+1} \oplus S_2 \oplus \ldots \oplus S_{(n-1)} \quad (3)$$

In step 4, we ensure that K_{t+1} is even parity. If not, the last insignicant bit will be toggled to make it even parity. It also toggles the last bit of B_{t+1}, so that equation (3) is still valid. Finally, in step 5, share K_{t+1}, between two shares $S_1 \oplus S_n$ by Algorithm 2 with input K_{t+1}.

S_0, $B_{t+1} = S_1 \oplus S_2 \ldots S_{(n-1)} \oplus S_n$. Further more, each blocks $S_1, S_2, \ldots, S_n$ is a POB(t +1, $\lfloor \frac{t+1}{2} \rfloor$) number.

Example 2 :

For a (5, 5) threshold scheme, secret B = 101101110 is taken.

By step 1, the extended string is, B_{t+1} of length 10 is 10110111 00

Randomly assign ve 1s and ve 0s to 3 rows $\{S_2, S_3, S_4\}$ in S. Therefore,

S_2 = 1011000101,

S_3 = 0101010110, and

S_4 = 1100101010.

Step 3. Computes K = 10011001 01, and In Step 5., 10011001 0 is split into

S_1 = 1010110010, and

S_5 = 0011010110.

All the 5 shares are listed below:

S_1 = 1010110010,

S_2 = 1011000101,

S_3 = 0101010110,

S_4 = 1100101010, and

S_5 = 0011010110.

Recovery: Computes $S_1 \oplus S_2 \oplus S_3 \oplus S_4 \oplus S_n$, and get B_{t+1} = 10110111 01.

Deleting the last bit of B_{t+1}, we get the secret as B_1 = 10110111 0.

3. Security Analysis

In this section, we discuss the security of the proposed scheme. In order to show the security of the uniform 2 out of 2 construction, suppose an illegal user gets one of the two shares. Lemma 3 shows guessing the secret correctly is very difcult.

Lemma 3 With only one share, the probability of guessing the shared secret correctly in a uniform construction is $\binom{t+1}{\lfloor \frac{t+1}{2} \rfloor}^{-1}$.

Proof : In a uniform construction, it is easy to observe that each share contains $\lceil \frac{t+1}{2} \rceil$ 1s. There are $\binom{t+1}{\lfloor \frac{t+1}{2} \rfloor}$ many variations for a block, and the probability of guessing one block correctly is $\binom{t+1}{\lfloor \frac{t+1}{2} \rfloor}^{-1}$. Hence the probability of an illegal user, who has only one share, guessing the shared secret is $\binom{t+1}{\lfloor \frac{t+1}{2} \rfloor}^{-1}$.

In order to show the security of an *n* out of *n* uniform construction, suppose there are fewer than *n* participants cooperating to guess the shared secret. Lemma 4 shows that even though there are *n-1* participants cooperating, the probability of guessing the shared secret correctly is still very low.

Lemma 4 : The probability of guessing the shared secret correctly in a uniform construction is $\binom{t+1}{\lfloor \frac{t+1}{2} \rfloor}^{-1}$, if only n - 1 shares are used to guess the share.

Proof : The proof is similar to that of Lemma 3.

Conclusions

We have presented a secret sharing scheme, in which the size of a share is just one bit more than the original secret size.

REFERENCES

1. Adi Shamir, *"How to Share a Secret"*, Communications of the ACM, Vol. 22, No. 11, PP. 612-613, Nov. 1979.
2. C. Asmuth and J. Bloom, *"A Modular Approach to Key Safeguarding"*, IEEE Transactions on Information Theory, Vol.IT-29, No.2, PP. 208-210, 1983.
3. G. Ateniese, C. Blundo, A. D. Santis and D. Atinson, *"Constructions and Bounds for Visual Cryptography"*, Proceedings 23rd International Colloquium on Automata Languages and Programming (ICALP '96), 1099, PP. 416-428, 1996,
4. G. Ateniese, C. Blundo, A. D. Santis and D. Atinson, *"Visual Cryptography for General Access Structures"*, Information and Computation, Vol. 129, No.2, PP. 86-106, 1996.
5. J. Benaloh, *"Secret Sharing Homomorphisms - Keeping Shares of a Secret Secret"*, In Advances in Cryptology - CRYPTO '86, A. M. Odlyzko, Ed. Vol. 263 of Lecture Notes in Computer Science, PP. 251-260, Springer-Verlag, 1987.
6. J. C. Benaloh and J. Leichter, *"Generalized Secret Sharing and Monotone Functions"*, Proceedings of Crypto '88, Advances in Cryptology, Lecture Notes in Computer Science, Vol. 403, S. Goldwasser, Ed., Springer-Verlag, Berlin, PP. 27-35, 1990.
7. M. Bertilsson, I. Ingemarsson, *"A Construction of Practical Secret Sharing Schemes using Linear Block Codes"*, In Proceedings AUSCRYPT '92, Springer Lecture Notes in Computer Science, Vol. 718, PP. 67-79, 1993.
8. G. R. Blakley, *"Safeguarding Cryptographic keys"*, Proceeding of AFIPS 1979 National Computer Conference, Vol. 48, New York, NY, PP. 313-317, June 1979.
9. B. Blakley, G. R. Blakley, A. H. Chan and J. L. Massey, *"Threshold Schemes with Disenrollment"*, Lecture Notes in Computer Science 740, PP. 546-554, 1993.
10. C. Blundo and D. R. Stinson, *"Anonymous Secret Sharing Schemes"*, Discrete Applied Mathematics, 77, PP 13-28, 1997.
11. E. F. Brickell, *"Some ideal secret sharing schemes"*, Journal of Combin. Math. and Commbin. Comput. No. 9, PP. 105-113, 1989.
12. R. M. Capocelli, A. De Santis, L. Gargano and U. Vaccaro, *"On the size of shares for secret sharing schemes"*, Journal Cryptology No. 6, PP. 157-168, 1993.
13. C. Chang, C. Tsait and T. Chen *"A New Scheme for Sharing Secret Colour Images in Computer Network"*, Proceeding of International Conference on Parallel and Distributed Systems, PP. 21-27, July 2000.
14. S. Droste, *"New Results on Visual Cryptography, Advances in Cryptology-CRYPTO'96"*, Lecture Notes in Computer Science, Vol. 1109, PP. 401-415, 1996.
15. R. Hwang and C. Chang, *"Some Secret Sharing Schemes and their Applications"*, Ph.D. dissertation of the Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan, 1998.
16. M. Ito, A. Saito and T. Nishizeki, *"Secret Sharing Schemes Realizing General Access Structure"*, Proceeding of IEEE Global Telecommunications Conference, Globecom 87, Tokyo, Japan, 1987, PP. 99-102, Journal version: Multiple Assignment

Scheme for Sharing Secret, Journal Cryptology, Vol 6, No. 6, PP. 15-20, 1993.

17. E. D. Karnin, J. W. Greene and M. E. Hellman, *"On Secret Sharing Systems"*, IEEE Transactions on Information Theory, Vol.IT-29, No. 1, PP 35-41, Jan 1983.

18. S. Kothari, *"Generalized Linear Threshold Scheme"*, Proceedings Crypto '84, Santa Barbara, CA (Aug 1984), 231-241. Published as Advances in Cryptology, ed. by Blakley and D. Chaum in Lecture Notes in Computer Science, Vol. 196, ed. by G. Goos and J. Hartmains, Springer-Verlag, New York 1985.

19. K. M. Martin, *"New Secret Sharing Schemes fron Old"*, Journal of Combin. Math. and Combin. Comput. No. 14, PP 65-77, 1993.

20. M. Mignotte, *"How to share a secret"*, Cryptography Proceedings of the Workshop on Cryptography, Burg Feuerstein, 1982, Volume 149 of LNCS, PP. 371-375 Springer-Verlag, 1983.

21. Moni Naor and Adi Shamir, *"Visual Cryptography"*, Advances in cryptology- EURO-CRYPT94, Lecture Notes in Computer Science, Vol. 950, PP. 1-12, 1995.

22. S. J. Phillips and N. C. Phillips, *"Strongly Ideal Secret Sharing Schemes"*, J. Cryptology, Vol.5 PP. 185-191, 1992.

23. A. Shamir, *"How to Share a Secret"*, Communications of the ACM, Vol. 22, No. 11, PP. 612-613, Nov. 1979.

24. G. J. Simmons, W. Jacjson and K. Martin, *"The Geometry of Shared Secret Schemes"*, Bulletin of ICA Vol. 1, PP. 71-88, 1991.

25. D. R. Stinson and S. A. Vanstone, *"A combinatorial approach to threshold schemes"*, SIAMJ. on Discrete Mathematics, 1(2):230-236, 1988.

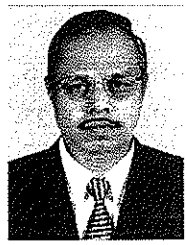
26. D. R. Stinson, *"An Explication of Secret Sharing Schemes"*, Designs,Codes and Cryptography, Vol. 2, PP 357-390, 1992.

27. M. Tompa and H.Woll, *"How to share a Secret with Cheaters"*, Journal of Cryptography, Vol.1, No.2, PP 133-138, 1988.

28. E. Verheul and H. V. Tilborg, *"Constructions and Propertics of k out of n Visual Secret Sharing Schemes"*, Designs, Codes and Cryptography, Vol. 11 No.2, PP. 179-196, 1997.

Author's Biography

A Sreekumar received the M. Tech degree in Computer Science from I.I.T. Madras in the year 1992. Currently he is working as a Lecturer at Cochin University of Science and Technology. He had 16 years of teaching experience



Dr. Babusundar received the M. Tech and Ph.D Degrees from Cochin University and working as Professor of Computer Applications in CUSAT. He had 26 years of teaching experience and his area of interest is Fuzzy logic Applications, ArticialIntelligence, Multimedia and Cryptography.