Diffie–Hellman Type 2D Key Exchange Scheme Using 2D-Convolution

Priya Nandihal and Bhaskara Rao.N

Dayananda Sagar College of Engineering, Bangalore. India.
talk2priya.nandihal@gmail.com
bhaskararao.nadahalli@gmail.com

Abstract— **A 2D Diffie–Hellman type key exchange method is presented. This new method uses 2D discrete convolution process to provide a secure shared 2D key between two users. It can be extended for more than 2 users.**

Keywords— **2D key, key exchange, 2D discrete convolution, image as a key.**

I. Introduction

The Diffie – Hellman [1] key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

In symmetric key cryptography keys are large sized binary numbers. But in the proposed method, the keys are 2D matrices which are represented by 2D images. Several methods have been already proposed [2],[3],[4] for 2D keys. In this paper, 2D discrete convolution operations are used to manipulate the matrices to generate the shared 2D secret key. This method is versatile and can be used for multi user common secret key sharing.

II. Terms, Definitions And Assumptions

All the entities participating in the scheme are 2D matrices whose elements are in the range, 0 to 255 (*uint8*). They in turn represent the corresponding grayscale images. These are processed to generate the public keys and the shared secret key.

A. Symbols and Terms

Alice and Bob are the two users communicating over an unsecured channel, who want to share a secret key.

1) Private Keys: P and Q are the private keys of Alice and Bob respectively. P and Q are 2D matrices of size M_P x N_P and M_Q x N_Q respectively. Alice can choose her own P and Bob can choose his own Q. The matrices P and Q are independent of each other.

2) Base Matrix: G is the base matrix known to both Alice and Bob. It is in the public domain. It can be obtained say by reading the well known image 'Leena' or by any other method. The size of G is m_G x n_G. Base matrix G is used to generate the public keys of Alice and Bob.

3) Public Keys: Matrices R and T are the public keys of Alice and Bob respectively. The sizes of R and T are M_R x N_R and M_T x N_T respectively. R is obtained by the discrete convolution of G and P, while T is obtained by the discrete convolution of G and Q.

4) Shared Secret Key: The shared 2D secret key is designated by matrix S. The size of S is M_S x N_S
The generation of all keys will be described in section III.

B. Main Operation

The main operation used in this scheme is 2D Discrete Convolution. Discrete Convolution is a widely used technique in image and signal processing applications [5],[6],[7].

*1) **Definition of 2D Discrete Convolution:*** Let A and B be two discrete 2D functions. Then the two-dimensional convolution of A and B is defined as,

$$C(m,n) = \sum_{i=-\infty}^{\infty}\sum_{j=-\infty}^{\infty} A\,(i,j) * B(m-i,n-j) \qquad (1)$$

When A and B are 2D matrices of sizes M_A x N_A and M_B x N_B with starting indices (1, 1) instead of (0, 0) for each matrix, the 2D convolution equation is rewritten as,

$$C(m,n) = \sum_{i=-\infty}^{\infty}\sum_{j=-\infty}^{\infty} A\,(i,j) * B(m+1-i,n+1-j) \qquad (2)$$

Here, C(m, n) is the value of C at indices m and n.

In Eq. (2), the range of i and j are so chosen that the indices of A and B are within their allowed range. That is, the row index for A is from 1 to M_A and for B it is from 1 to M_B. Similarly, column indices for A and B vary from 1 to N_A and 1 to N_B respectively. Under these conditions, i and j should obey the following constraints. From the consideration of the indices of A(i, j),

$$1 \le i \le M_A \qquad (3)$$

and

$$1 \le j \le N_A \qquad (4)$$

Similarly from the consideration of B(m+1–i, n+1–j),

$$1 \le (m+1-i) \le M_B \qquad (5)$$

and

$$1 \le (n+1-j) \le N_B \qquad (6)$$

From Eqs. (3) and (5), the lower limit of i is given by,
$i \ge 1$ and $i \ge (m+1-M_B)$ That is,

$$i_{lower} = \max(1, m+1-M_B) \qquad (7)$$

Similarly from Eqs. (3) and (5),

$$i_{upper} = \min(M_A, m) \quad (8)$$

Similarly, From Eqs. (4) and (6), limits on j are,

$$j_{lower} = \max(1, n+1-N_B) \quad (9)$$

$$j_{upper} = \min(N_A, n) \quad (10)$$

The summation of Eq. (2) is carried out subjected to the constraints specified by Eqs. (7), (8), (9) and (10). Then substituting lower and upper limits for i and j, Eq. (2) becomes,

$$C(m,n) = \sum_{i=i_{lower}}^{i_{upper}} \sum_{j=j_{lower}}^{j_{upper}} A(i,j) * B(m+1-i, n+1-j) \quad (11)$$

the size of C represented by M_C x N_C would be,

$$(M_C \text{ x } N_C) = ((M_A + M_B - 1) \text{ x } (N_A + N_B - 1)) \quad (12)$$

The convolution of A and B as given by Eq. (11) is also written as,

$$C = A \bullet B \quad (13)$$

The symbol● is used as the convolution operator. The convolution given by Eq. (11) or (13) is also represented by the *conv2* function as [5],

$$C = \text{conv2}(A,B) \quad (14)$$

conv2(A, B) computes the two-dimensional convolution of matrices A and B.

*2) **Properties of 2D convolution:*** Properties of 2D convolution are similar to 1D convolution properties [8]. Convolution operations are associative and commutative These properties are derived from the definition of 2D convolution given by Eq.(1). Thus for any three matrices C, D and E, associative property yields,

$$(C \bullet D) \bullet E = C \bullet (D \bullet E) \quad (15)$$

For any two matrices, the commutative property yields,

$$C \bullet D = D \bullet C \quad (16)$$

III. Common Secret Key Generation

Basic approach

We use function conv2 along with private keys P, Q and base matrix G as described in section II, to generate the secret common key. The steps to generate the key are as follows.

1. User Alice chooses her private key P which is a matrix of unsigned integers in the range 0 to 255. The size of matrix P is M_P x N_P. It represents a gray scale image.

2. Alice's public key R is obtained as,

$$R = \text{mod}(G \bullet P, 256) \quad (17)$$

Since the elements of G and P are positive integers, the convolution sum G●P is also a matrix of positive integers. we need to keep the resulting elements in the range 0 to 255 so that G●P also represents an image. Therefore *modulo 256* operation is applied to G●P to restrict its elem ents in the range 0 to 256. Another important purpose of modulus operation is to make R a *one way function*. That is, by knowing G and R, P cannot be solved in reasonable time. After the convolution and the modulus operation, the resulting matrix R of Eq. (17) has its elements in the range 0 to 255. The size of R is,

$$(M_R \text{ x } N_R) = ((M_G + M_P - 1) \text{ x } (N_G + N_P - 1)) \quad (18)$$

3. R is sent to user Bob over the unsecured channel.

4. User Bob chooses his private key Q.

5. Bob's public key T is obtained as,

$$T = \text{mod}(G \bullet Q, 256) \quad (19)$$

The size of T is,

$$(M_T \text{ x } N_T) = ((M_G + M_Q - 1) \text{ x } (N_G + N_Q - 1)) \quad (20)$$

6. T is sent to user Alice over the unsecured channel.

7. User Bob, having received R, generates the secret key S_B as,

$$S_B = \text{mod}(R \bullet Q, 256) \quad (21)$$

8. User Alice, having received T, generates her secret key S_A as,

$$S_A = \text{mod}(T \bullet P, 256) \quad (22)$$

Now, it can be shown that the common secret key for user Alice and Bob is $S = S_A = S_B$. Substituting for R from Eq. (17) in Eq.(21),

$$S_B = \text{mod}(\text{mod}(G \bullet P, 256) \bullet Q, 256) \quad (23)$$

From the basic properties of the modular algebra and the associative property of convolution, Eq. (23) can be rewritten as,

$$S_B = \text{mod}(G \bullet P \bullet Q, 256) \quad (24)$$

Similarly, from Eqs.(19) and (22),

$$S_A = \text{mod}(\text{mod}(G \bullet Q, 256) \bullet P, 256)$$

From this we get,

$$S_A = \text{mod}(G \bullet Q \bullet P, 256) \quad (25)$$

By the commutative property of 2D convolution,

$$P \bullet Q = Q \bullet P \quad (26)$$

From Eqs.(24),(25) and (26),

$$S_A = S_B = \text{mod}(G \bullet Q \bullet P, 256) = \text{mod}(G \bullet P \bullet Q, 256) \quad (27)$$

Calling this as S, the shared secret key is,

$$S = S_A = S_B = \text{mod}(G \bullet P \bullet Q, 256) \quad (28)$$

Cryptanalysis of the proposed method

Here, modulus 256 operation makes the 2D convolution a one way function. Consider the convolution, R = G●P. By knowing R and G, the value of P can be determined by solving the set of simultaneous equations given by G●P = R. But when modulus is introduced as, R = mod(●G P, 256), the information in R is reduced compared to its pre modulus value.

Therefore it is very hard to determine P by knowing G and R after the modulus operation. Thus modulus, operation protects the private keys from hackers.

IV. ENCRYPTION AND DECRYPTION

We can use the secret key as generated in section III to encrypt and decrypt digital 2D images. The size of the 2D key generated and the image to be encrypted should be same. The function *bitxor* is used for encryption and decryption operations. Let T be the test image and T_A be its encrypted format .The steps to encrypt/decrypt T are as follows.

1. Alice encrypts the image T with her 2D secret key S_A as,

$$T_A = \text{bitxor}(T, S_A) \qquad (29)$$

2. Alice sends the encrypted image T_A over an unsecured channel to Bob.
3. Bob receives T_A and decrypts the image using his 2D secret key S_B as,

$$T = \text{bitxor}(T_A, S_B) \qquad (30)$$

T is the original image recovered by Bob after decryption.

V. EXPERIMENTAL RESULTS

In the Matlab experiment, G is the grayscale base image. Here, G is obtained by reading the grayscale image *Leena* whose size is 225 x 225. The image G is shown in Fig. 1. The private keys P and Q are random matrices of size 10x10 with values in the range 0 to 255. Fig.2. shows the convoluted image R=mod(G●P, 256) which is the public key of Alice whose size is 234 x 234. The common shared key is given by eq. (21) as S_B = mod(R●Q, 256). The size of S_B is 243 x 243. It is shown in Fig 3. The expression, S_A given by Eq. (22) is found to be exactly same as S_B. T is the grayscale test image of size 225 x 225 used for encryption using the secret 2D key. It is shown in Fig. 4. The size of T is resized to 243x243 to match the size of S_A or S_B. The encrypted image designated as T_A is shown in Fig. 5. Matlab function conv2(A, B) is used for calculating the 2D convolutions. Matlab function mod(X,Y) is used for modulus calculation.

Fig.1 Base Image G

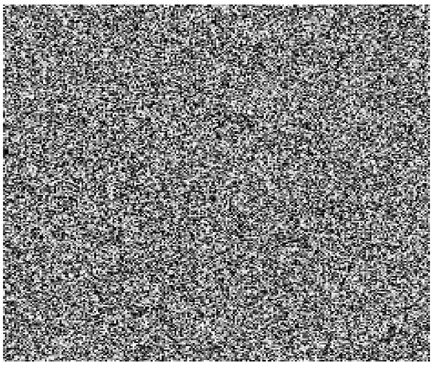

Fig.2. convoluted image R

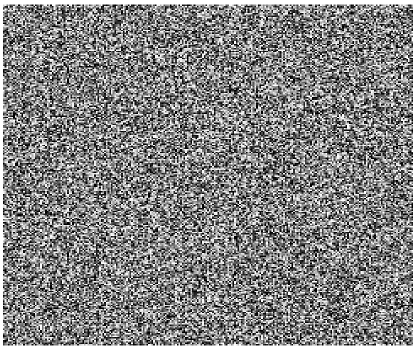

Fig 3. Double Convoluted Image S_B

Fig 4. Test image T

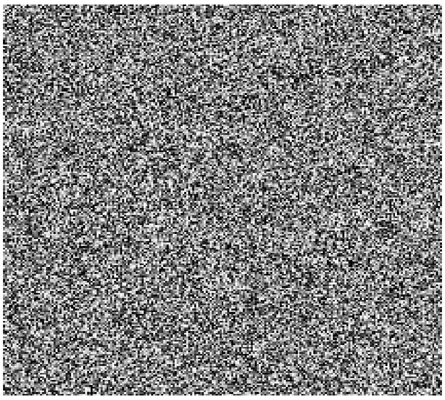

Fig 5. Encrypted image T_A

VI. Conclusion

This paper presents a new scheme of generating Diffie-Hellman type 2D common keys. Since the secret key is 2D matrix, it can be used for encryption/decryption of document images and other block oriented data. The size of the key can be very large. For example a 2D key image of size 256x256 has a size of 65,536 bytes. For generating the various matrices and for convolution calculations, Matlab Image Processing Toolbox can be effectively used for easy coding.

As the size of common secret key size is large the chances of key theft and discovery by unauthorized outsiders is very low. This scheme can be easily extended to more than two users using successive convolution. The encryption decryption technique using 2D keys can be extended to videos.

References

[1] William Stallings, Cryptography and Network Security Principles and Practices. Fourth Edition. Pearson Education. 2006.

[2] Yicong Zhou, Karen Panetta and Sos Agaian, “Image Encryption Using Binary Key-images”, Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics San Antonio.

[3] Kok-Wah Lee “High-Entropy 2-Dimensonal Key Input Method for Symmetric and Assymetric Key Cryptosystems”, IJCEE,Vol 1,April 2009.

[4] Priya Nandihal and Bhaskara Rao N. “2D Key Exchange Scheme Using Morphological Dilation” IJCSET,Vol2,March 2012.

[5] R.C. Gonzalez and R.E. Woods, “Digital Image Processing”, third Edition. Pearson Education. 2009.

[6] From Wikipedia, the free encyclopedia. en.wikipedia.org/wiki /convolution.

[7] www.mathworks.com/help/toolbox/images/ref/conv2.html.

[8] Discrete Time signals and systems. www.pearsonhighered.com /assets/hip/us/hip_us.../0131988425.pdf.