GÜVENLİ HABERLEŞME PROTOKOLLERİNDE GÖRÜNTÜ UZAYININ KULLANIMI

Alper UĞUR[1] Murat AYDOS[2]

[1,2] Pamukkale Üniversitesi Bilgisayar Mühendisliği Bölümü
Morfoloji Binası Kınıklı Kampüsü, 20017 DENİZLİ

[1]e-posta: augur@pamukkale.edu.tr [2]e-posta: maydos@pamukkale.edu.tr

Anahtar sözcükler: pseudo-random sayı üreteçleri, Görüntü İşleme, Hash fonksiyonları,Oturum anahtarı

ABSTRACT

This paper presents heuristic application fields of image space in the cryptographic secure communications. As it is known, image processing are already being used in secure communication and data hiding (watermarking) technologies. But all these applications use images and pictures as envelopes of valuable data. We let them play in real game as pivot.

The purposed opinion is based on procuring essential cryptographic data from images by optical diversity and pixel processing. The obtained data can be used in mutual authentication and key establishment protocols, which are the base of secure transactions. Achieved statistics and simulations indicates that image space forms a large and unpredictable data set and may re-donate diverse data to the cryptographic secure communication protocols.

1.GİRİŞ

Güvenli haberleşmenin temelini teşkil eden kriptografide asal sayılar, Galoi alanlar, elliptik eğriler gibi birçok matematiksel veriler işlenmekte ve kullanılmaktadır. Bunun yanında watermarking, filigran benzeri yöntemlerle de görüntü içine veriler fark edilmesi engellenerek yerleştirilmekte ve bunlarla görüntünün kimlik doğrulaması yapılmakta ya da görüntü kapalı bir zarf gibi kullanılarak gizlenen verinin güvenli iletimi sağlanmaktadır.

Bu bildiride görüntünün güvenli haberleşmede kullanılabileceği başka yöntemler sunulacak ve bunlar ile ilgili yaptığımız analizler ortaya konulacaktır.

Bu yöntemler; haberleşmede gerek protokol kurulmadan yapılan sınama-doğrulama aşamaları gerekse veri bütünlüğünün sağlanmasında kullanılan rasgele sayı üretimi ve oturumun güvenliğini sağlayan oturum anahtarı üretimidir.

2.SÖZDE (pseudo) RASGELE SAYILAR

Sistemlerde ve hemen hemen her derleyicide hali hazırda bulunan rasgele sayı üreteçlerinin büyük olasılıkla rasgele sayılar üretememesi ve bu sayıların kriptografik olarak kesinlikle güvenli olmadığı bilinmektedir. Bilgisayarların deterministik yapısı sebebiyle üretilecek sayının gerçek bir rasgele sayı olması beklenemez. Bunun yerine kriptografi, ihtiyacını sözde (pseudo) rasgele sayılardan karşılamaktadır.

Bir sayı serisinin sözde rasgele sayı serisi olması için

1- Sayının rasgele görünümünde olması
2- Bir sonraki sayının tahmin edilemez olması
3- Tekrar üretilemez olması

özelliklerini taşıması gerekir. [1]

Hash fonksiyonlarının büyük olasılıkla farklı çıkış vermeleri bu fonksiyonların rasgele sayı üretiminde kullanılabileceğini göstermiştir.[2]

Bu fonksiyonlar için kullanılacak verinin görüntü serilerinden eldesi yukarıda sıralanan özelliklerin sağlanmasına katkıda bulunacaktır.

3.KULLANILAN YÖNTEM

Kullandığımız yöntem görüntü uzayından veriyi, görüntü yüzeyinin piksellere doğrusal operatör matrisi ile ayrılarak her bir pikselde bulunan renk kodlarının işlenmesi ile sağlamaktadır. Daha sonra elde edilen bu veriler standartlaşmış hash fonksiyonları için (yapılan çalışmada hash fonksiyonu olarak FIPS 180-2'ye uygun olarak kodlanan SHA–256 kullanılmıştır) girdi oluşturarak sözde rasgele sayı serisini meydana getirmektedir. Bu yöntem Şekil-1'de şematik olarak gösterilmiştir.

4.GÖRÜNTÜLERİN ÇEŞİTLİLİĞİ VE OPTİK FARKLILIK

Görüntünün elde edilmesi kullanılan donanım ve yazılıma bağlı olarak veri farklılığı oluşturduğu gibi, içinde bulunduğu ortamında görüntünün özelliklerini değiştirdiği bir gerçektir. Işığın yüzeyden yansıyarak görüntüyü oluşturması, donanımlar arasındaki çözünürlük farkları, ortamın aydınlığı, optik açı farkları görüntüyü dolayısıyla görüntüden elde edilecek veriyi etkileyen, değiştiren faktörlerdendir.

Kuramsal olarak fiziksel görüntüler sadece sonlu zaman aralıklarında gözlemlenebilirler. Buna bağlı olarak görüntü ışık fonksiyonu C(x,y,t,λ) gibi dört değişkenli bir fonksiyondur. Göreli kırmızı, yeşil, mavi (RGB) koordinat sistemi:
(x,y): uzaysal koordinat sistemi,
t: zaman
λ: dalgaboyu
$R(x,y,t)= \int^{\infty}_{0} C(x,y,t,\lambda)\, Rs(\lambda) d\lambda$
$G(x,y,t)= \int^{\infty}_{0} C(x,y,t,\lambda)\, Gs(\lambda) d\lambda$
$B(x,y,t)= \int^{\infty}_{0} C(x,y,t,\lambda)\, Bs(\lambda) d\lambda$
değerlerinden oluşur. [3]
Dolayısıyla görüntüler zamana ve ışık spektrumuna bağlı değişken yapıdadırlar.
Buna örnek olarak Tablo-1'de farklı zaman dilimlerinde aynı plandan alınan görüntülerin farklı verileri taşıdıkları ile ilgili çalışmanın sonuçları yer almaktadır.
Bunlara ek olarak cihazın bakış açısındaki küçük değişiklikler, görüntünün kısmi ya da bütünsel olarak işlem görmesi tek kaynaktan elde edilecek veri çeşitliliğini artırmaktadır.
Tüm bu bilgilerin ışığında, varolan bu veri çeşitliliği görüntü uzayının rasgele sayı serisi üretiminde kullanılmasını cazip kılmıştır.

5. RASGELE SAYI SERİSİ ÜRETİMİNDE GÖRÜNTÜ UZAYI

Bir tütsü yakılarak çıkacak dumandan rasgele bir görüntü kümesi oluşturulması amaçlanmıştır. Arka plan asgari veride azami performans araştırması için siyah renk ile kısıtlanmış, değişkenlik sadece hareketin rasgeleliği ile sınırlandırılmıştır. Bununla beraber daha öncede belirtildiği gibi ortam ışığı değişimi veya optik farklılığı görüntü çeşitliliğini ve önceden tahmin edilemezlik özelliğini pekiştirmektedir.
Intel PcCamera CS110 kullanılarak yakalanan 320X240 boyutundaki 4.06 sn.lik görüntü serisinden elde edilen 392 görüntü çerçevesi Şekil-2'de vurgulanan merkezde 100x100 lük bir dikdörtgensel alanda işlenmiş ve Tablo-2 ve Tablo-3'te sunulan sonuçlar elde edilmiştir.
392 verideki 0 biti değeri adedi: 50296 1 biti değeri adedi: 50312 olduğu hesaplanmıştır. Bu, bitlerin dağılımı ve rasgelelik için dengeli bir sonuçtur.
Üretilen sayının sıkıştırılamaması sözde rasgele sayılar için bekleneni vermektedir. Tablo-2'de onaltılık sayı sistemiyle sadece bir kısmı gösterilen veriler için, 0 ve 1'lerin dağılımını tüm sayı serileri bazında en yaygın sözde rasgele sayı testi olan Ki-kare istatistiksel testi uygulanmış *p* değeri 0,001'den küçük çıkması uygunluğu desteklemektedir. Ki-kare testi uyum, homojenlik ve bağımsızlık analizlerini içermektedir. Bu sonuç izlenen yöntemin hash fonksiyonunun özelliğini olumsuz etkilemediğini göstermiştir.
0.6 sn aralıklarla kaydedilen görüntülerin işlenmesi sonucunda üretilen veriler sözde rasgele sayı serilerinin özelliklerini taşıdığı gözlemlenmiştir.

Bu yolla elde edilecek verilerden haberleşme güvenliğinde kullanılan sınama-yanıt protokolünde gerekli olan rasgele sayının üretilmesinde kullanılabilinecektir. Bilindiği gibi sınama-yanıt protokolleri karşı tarafın kimliğinin gizli bilgisinin açığa çıkmadan doğrulanmasını sağlayan karşılıklı ileti alışverişidir. Zaman pulu kullanımı taraflara senkronize olma zorunluluğu gerektirdiğinden, bu alışverişte rasgele sayıların önceden tahmin edilemezliği ve tekrarlanmaması özelliklerinden faydalanılmaktadır. Kerberos, SESAME (aynı zamanda açık anahtarlı bir sistemdir) gibi gizli anahtara dayanan haberleşme protokollerinde üretilen sayı karşı tarafa gönderilir ve bu sayının şifrelenmesi beklenir. Eğer sayı ortak gizli anahtarla tekrar elde edilebiliyorsa kimlik doğrulanmış olur ve haberleşme başlangıcı tamamlanır. [4] İletişimdeki iki taraf arasındaki illegal üçüncü şahıs'ın (man-in-the-middle) trafikteki verileri tutması rasgele sayının gücüyle orantılı olarak faydasızlaşır.

6. ANAHTAR OLUŞTURMADA GÖRÜNTÜ UZAYI

Gizli anahtarlar üzerine kurulan protokollerin hemen hepsi anahtarın taraflara emin yollardan ulaştırılmış olduğu varsayımı ile başlar. Bu yöntemde de taraflara ulaştırılan görüntü havuzlarının gizli kaldığı varsayılmıştır. Taraflar, sistem tarafından belli aralıklarla güncellenen görüntü havuzlarından seçilen görüntülerden oluşturdukları rasgele sayılarla kimlik doğrulaması yaptıktan sonra belirlenecek koordinatlar arasında kalan yüzeyin işlenmesi ortak anahtarın elde edilmesini sağlayacaktır. Bu süreç Şekil-3'te şematik olarak gösterilmiştir.
Süreci açıklamak için kullanılan değişkenler:
A,B: taraflar
Rg: Görüntü havuzundan elde edilmiş rasgele sayı
k: gizli anahtar
kg^{1} : Görüntü havuzundan elde edilmiş yeni oturum anahtarı
E()k: gizli anahtara bağlı şifreleme
H(): hash (tek yönlü) fonksiyonu
ID: taraf kimliği
M: mesaj
(x_n,y_n) : işlem çerçevesi koordinatları
(x_0,y_0) : başlangıç koordinatları
(x_s,y_s) : bitiş koordinatları
Ig: Görüntü kimliği
F: Görüntü çereçeve fonksiyonu
anlamını taşır.

A, B'nin kimliğini sınamak için görüntü havuzundan yukarıda belirtilen yöntemle oluşturulan rasgele sayıyı gönderir. B bu sayıya kendi kimliğini ve gerekli diğer bilgileri ekleyip hashini alarak A'ya gönderir. A elindeki bilgilerin hashini alarak karşılaştırma yapar. Kimlik doğrulanmışsa görüntü havuzundan seçilen bir görüntü tanımlayıcısını, çerçeve koordinatlarını ve isteğe bağlı F fonksiyonunu yollar. Ortak olarak elde edilen anahtar ile oturum başlar.

F fonksiyonu koordinatlar arasındaki alandaki doğrusal operatör matrisinden gerekli verinin farklı şekillerde oluşturulmasını sağlamak için düşünülmüştür. Böylece veriler sadece dikdörtgensel alanlardan değil eğrisel alanlardan da elde edilecek ve yöntem karmaşıklığı dış etkenlere karşı artırılacaktır.

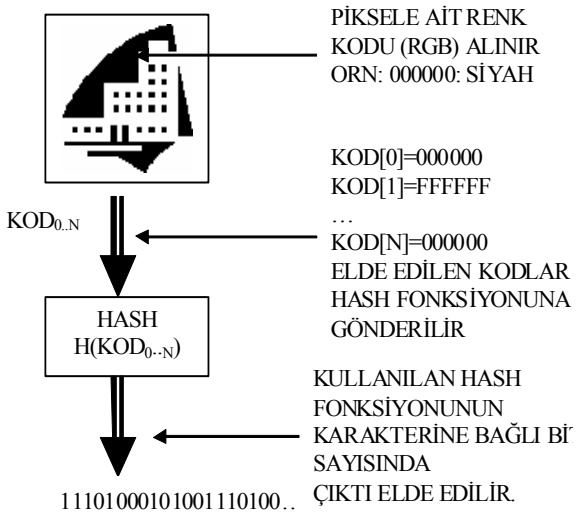
7. SONUÇLAR

Daha öncede bahsedildiği gibi görüntü uzayının büyüklüğü çeşitliliği de getirecektir. Ama bilinmelidir ki elde edilecek anahtar kullanılan hash fonksiyonunun çıkış uzunluğuna bağlıdır. Örneğin SHA-256 kullanıldığında taranması gereken anahtar uzayı 2^{256} olacaktır.

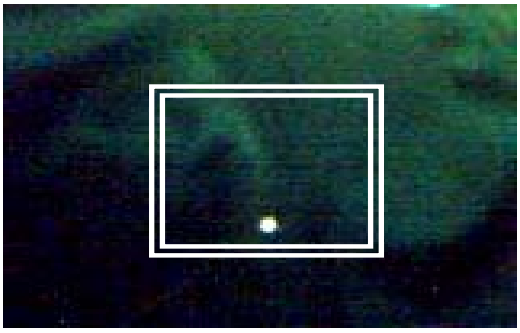
Bu şekilde bir rasgele sayı veya anahtar üretimi birkaç saniye de olsa uzun süreceği için işlemin protokol başlangıcında yapılması önerilmektedir. Bununla birlikte daha önceden elde edilmiş rastgele sayılar bir havuzda tutulabilir. Bu havuzun boyutu kullanılan sistem ve cihazlarla yakından bağlantılıdır. Küçük elektronik akıllı cihazlar (Smart-Cell-Phone, PDA, etc.) gibi cihazların gücü ve hafızası düşük olacağından havuzun boyutu sınırlanmalıdır.

Bu çalışmada kriptografik güvenlik uygulamalarında hayati önem taşıyan rastgele sayıların üretilmesinde alışılagelmiş metotlardan farklı olarak görüntü uzayının kullanılması işlenmiştir. Tablolarda verilen sonuçlar göstermektedir ki bu yöntemle elde edilen rastgele sayılarının standartlara uygunluk testini geçmiştir.

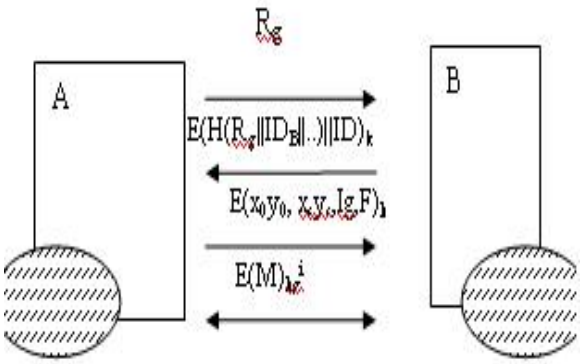
Makalede verilen kimlik tanıma ve anahtar seçimi protokolü (mutual authentication & key agreement protocol) sadece örnek teşkil etmesi açısından eklenmiştir. Bu protokolün tüm ataklara karşı direnci bu çalışmada değerlendirilmemiştir.



Şekil-1 Görüntüden rasgele sayı üretimi



Şekil-2 Görüntü çerçevesi ve işlem alanı



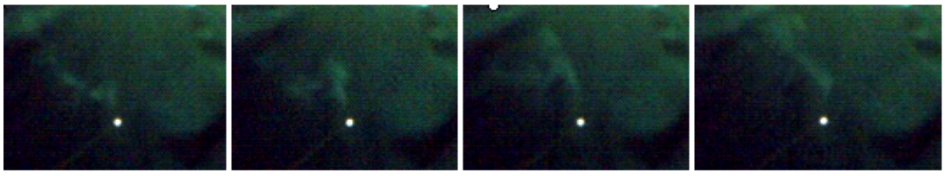
Şekil-3 Oturum süreç şeması

[1] Schneier B., Applied Cryptography, John Wiley & Sons. Inc, 1996
[2] Federal Information Processing Standards Publication 180-2, 2002
[3] Pratt W.K. Digital Image Processing: PIKS Inside, Third Edition, John Wiley & Sons. Inc, 2001
[4] Menezes A, Handbook of Applied Cryptography, CRC Press, 1997

Tablo-1 Tek renkli düz bir zeminden 13:00 ile 17:00 arası alınan görüntülerden elde edilen değerler

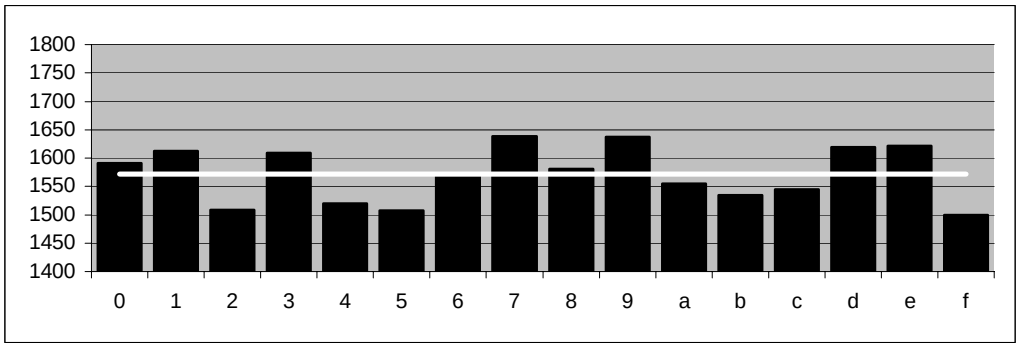
t	Değerler (onaltılı sistem)							
1	4adcd1be	2d103fd0	16cd47b5	eda83c4d	74834cb9	aeeb8b13	ce36011a	8b95ea4b
2	b41b25b3	c51c6730	affefe0e	2f544c01	da6287ff	093c862b	7e58fbea	e34c760e
3	b0ba6a76	ffd2307d	32fb0105	1e6c326c	0c0bc745	6fb994c4	b8b1f1f3	434c7f53
4	c7956e76	fcf21354	572e2376	98db2fd3	b2f33c35	ee2ef921	81243ae7	3c72e4d7
5	b6bc505e	d46cfad0	021f46e6	7a11d6a0	e81364da	ed39f2f9	1144e03f	2fb4a0bd
6	9c5a5e69	397a11f1	ad1f4bcd	f65c194e	5dc65334	d708d1a4	52009b3f	2b5dbb21
7	a57875de	aa343a8a	d35dd557	d16704df	fc83a646	a63f6638	b72574c9	e6243898
8	5e6a0b04	9ccb3d03	1097ad3e	315f4760	5a019f11	6c9ff5c3	4f0934af	686d2e62
9	5e2312ca	dd7af0eb	3e4e4775	784e942f	e7e61e41	8216ad3b	9d6be666	5e76f258
10	d4967893	c8e7c88c	b017edea	43a458dd	314b6218	0a490114	14b1c993	0000f17d
11	d0fc25f3	f2573000	306e76cd	8ac8b6b9	c6891a55	ac156f01	e1db73b1	ffe94281
12	b4b7cfe9	507374401	72361484	3d744e80	4db3001a	5bf0f91b	1a36374b	4aae07c

Tablo-2 Örnek görüntüler ve hash değerleri



	126	127	128	129
126	6cf0a181 b8a29a65	8164028a bbfe05cd	ddb8bea1 63334947	57324b43 efe5e0e3
127	f763c18d 76f10318	8c7635c5 9159b4d6	f62dcc50 6a98ff24	263b5f8a c6832f88
128	104f6803 0f454606	ea9041df 4786d10d	8ecc7cef 07ef52c1	7d686137 89c8d4f6
129	f4d9f9b9 33318eb6	f72d3aa2 97532dfc	ac25ac81 0ab2dd95	90a4ca1a ccdf8dba

Tablo-3 Elde edilen verilerin onaltılık sistemdeki dağılımı



Tablo 4 Verilerin ikili sistemdeki dağılımı

0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
130	126	140	116	127	129	135	121	127	129	127	129	116	140	125	131
132	124	141	115	134	122	126	130	132	124	133	123	131	125	143	113
126	130	128	128	140	116	114	142	123	133	126	130	127	129	130	126
122	134	123	133	131	125	132	124	136	120	145	111	135	121	145	111
129	127	115	141	134	122	121	135	119	137	135	121	132	124	119	137
149	107	132	124	125	131	131	125	121	135	120	136	111	145	119	137
126	130	125	131	119	137	115	141	119	137	115	141	134	122	127	129
131	125	136	120	128	128	116	140	123	133	123	133	131	125	132	124
129	127	133	123	130	126	130	126	122	134	137	119	124	132	140	116
120	136	138	118	124	132	136	120	117	139	139	117	137	119	126	130
111	145	147	109	135	121	121	135	126	130	128	128	133	123	117	139
138	118	127	129	117	139	126	130	136	120	125	131	137	119	144	112
137	119	128	128	118	138	135	121	125	131	129	127	132	124	126	130
129	127	124	132	132	124	124	132	128	128	140	116	132	124	114	142
133	123	126	130	143	113	130	126	130	126	111	145	129	127	123	133
138	118	132	124	129	127	121	135	122	134	125	131	116	140	133	123
134	122	128	128	140	116	120	136	119	137	131	125	115	141	127	129
132	124	127	129	118	138	135	121	134	122	139	117	135	121	131	125
120	136	128	128	137	119	122	134	137	119	126	130	135	121	141	115
119	137	133	123	117	139	126	130	142	114	118	138	131	125	126	130
130	126	130	126	148	108	143	113	117	139	126	130	122	134	123	133
118	138	131	125	134	122	138	118	129	127	125	131	116	140	137	119
120	136	130	126	120	136	118	138	134	122	133	123	119	137	139	117
135	121	128	128	142	114	125	131	123	133	124	132	125	131	125	131
130	126	131	125	139	117	117	139	138	118	128	128	143	113	133	123
123	133	112	144	113	143	135	121	115	141	127	129	130	126	130	126
140	116	127	129	144	112	126	130	119	137	120	136	115	141	134	122
131	125	124	132	139	117	126	130	136	120	130	126	134	122	125	131
122	134	130	126	130	126	126	130	118	138	120	136	113	143	127	129
141	115	129	127	128	128	127	129	121	135	130	126	128	128	131	125
120	136	137	119	134	122	131	125	131	125	134	122	130	126	121	135
134	122	129	127	121	135	128	128	123	133	115	141	127	129	141	115
115	141	122	134	124	132	119	137	135	121	128	128	138	118	120	136
139	117	126	130	122	134	114	142	131	125	140	116	116	140	133	123
138	118	111	145	128	128	125	131	129	127	129	127	130	126	125	131
133	123	118	138	127	129	120	136	123	133	125	131	120	136	135	121
122	134	129	127	124	132	133	123	127	129	127	129	129	127	113	143
119	137	125	131	131	125	118	138	122	134	134	122	142	114	125	131
126	130	129	127	133	123	122	134	127	129	133	123	120	136	132	124
128	128	121	135	134	122	126	130	132	124	123	133	126	130	125	131
140	116	126	130	125	131	133	123	106	150	134	122	130	126	126	130
133	123	129	127	142	114	122	134	122	134	129	127	129	127	132	124
135	121	120	136	134	122	138	118	133	123	126	130	137	119	115	141
129	127	126	130	128	128	132	124	118	138	141	115	115	141	120	136
126	130	122	134	128	128	131	125	127	129	113	143	130	126	118	138
128	128	122	134	120	136	129	127	138	118	135	121	122	134	133	123
123	133	127	129	120	136	131	125	125	131	132	124	129	127	133	123
136	120	139	117	122	134	119	137	134	122	137	119	124	132	131	125
133	123	120	136	118	138	142	114	130	126	120	136	136	120	129	127