T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

ALFA KANALI İLE STEGANOGRAFİ

Yüksek Lisans Tezi

Tezi Hazırlayan:
Burcu ÜNLÜ

İstanbul, 2019

T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

ALFA KANALI İLE STEGANOGRAFİ

Yüksek Lisans Tezi

Tezi Hazırlayan:
Burcu ÜNLÜ

Öğrenci No:
160820027

Danışman:
Dr. Öğr. Üyesi Ediz ŞAYKOL

İstanbul, 2019

YEMİN METNİ

Yüksek Lisans Tezi olarak sunduğum **"Alfa Kanalı ile Steganografi"** başlıklı bu çalışmanın, bilimsel ahlak ve geleneklere uygun şekilde tarafımdan yazıldığını, yararlandığım eserlerin tamamının kaynaklarda gösterildiğini ve çalışmamın içinde kullanıldıkları her yerde bunlara atıf yapıldığını belirtir ve bunu onurumla doğrularım. 17/05/2019

Burcu ÜNLÜ

T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZ SAVUNMA SINAVI SONUÇ TUTANAĞI

Beykent Üniversitesi
Fen Bilimleri Enstitüsü Müdürlüğü'ne,

Aşağıda tez adı belirtilen yüksek lisans öğrencisi..160820027..no'lu Burcu Ünlü...'in 13/06/2019 tarihinde yapılan tez savunma sınavı[1] sonucunda..45. dakika süreyle sunduğu ve savunduğu tezi hakkında[2] oybirliğiyle, ..KABUL.. kararı verilmiştir.

Bilgilerinize saygılarımızla arz ederiz.

Anabilim Dalı : BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
Programı : BİLGİSAYAR MÜHENDİSLİĞİ
Tez Başlığı[3] : ALFA KANALI İLE JSTEGANOGRAFİ

Tez Sınav Jürisi	Öğretim Üyesi	İmza
Danışman :	Dr. Öğr. Üyesi Ediz ŞAYKOL	
Üye :	Prof. Dr. Gökhan DALKILIÇ	
Üye :	Dr. Öğr. Üyesi Atılay İLHAN	

---

[1] Jüri üyeleri, söz konusu tezin kendilerine teslim edildiği tarihten itibaren en geç bir ay içinde toplanarak öğrenciyi tez sınavına alır. Tez savunma sınav süresi en az 45, en çok 90 dakikadır. Jüri üyeleri, sınav öncesi yapılacak toplantıda, kendi aralarından danışman dışında bir üyeyi başkan seçer. Tez sınavı, tez çalışmasının sunulması ve bunu izleyen soru-cevap bölümünden oluşur. Tez sınavı, öğretim elemanları, lisansüstü öğrenciler ve alanın uzmanlarından oluşan dinleyicilerin katılımına açık ortamlarda gerçekleştirilir. Belirlenen günde yapılamayan jüri toplantısı, katılanların hazırladığı bir tutanakla enstitü yönetimine bildirilir. Bu durumda, jüri en geç on beş gün içinde toplanarak adayı tez savunma sınavına alır. (05 Ağustos 2017 tarihli 30145 sayılı Resmi Gazetede Yayınlanan Değişiklik-Madde 29-3)

[2] Tez sınavının tamamlanmasından sonra jüri, tez hakkında salt çoğunlukla "kabul", "düzeltme" veya "ret" kararı verir. Jüri başkanı, jüri üyelerince imzalanmış karar tutanağını, tez sınavını izleyen üç gün içinde ilgili enstitü yönetimine teslim eder. Tezi hakkında düzeltme kararı verilen öğrenci en geç üç ay içinde gerekli düzeltmeleri yaparak ve birinci fıkradaki usule göre tezini aynı jüri önünde yeniden savunur. Süresi içerisinde "düzeltme" savunmasına girmeyen öğrencinin enstitü ile ilişiği kesilir. (Beykent Üniversitesi Lisansüstü Eğitim ve Öğretim Yönetmeliği-Madde 29-4)

[3] İleride doğabilecek aksaklıkların engellenmesi için tezin başlığının yazılması gerekmektedir.

Adı ve Soyadı : Burcu ÜNLÜ
Danışman : Dr. Öğr. Üyesi Ediz ŞAYKOL
Türü ve Tarihi : Yüksek Lisans Tezi/2019
Alanı : Bilgisayar Mühendisliği
Anahtar Kelimeler : Steganografi, Alfa Kanalı ile Steganografi

ÖZ

ALFA KANALI İLE STEGANOGRAFİ

Bu çalışmada, Steganografi bilimi yöntemlerine yeni bir yöntem getirilmesi amaçlanmıştır. Bilinen bazı Steganografi yöntemleri üzerine incelemeler gerçekleştirilmiş ve güncel konular üzerinden teknikler açıklanmaya çalışılmıştır. Steganografi alanlarından bir tanesi olan görüntü ile mesajlaşma yöntemi üzerinde durulmuş ve bazı görüntülerde yer alan alfa kanalı üzerinden Steganografi gerçekleşebileceği gösterilmiştir. Görüntüler üzerinden gizli mesaj gönderimi esnasında ilgili resimde yer alan görüntünün de bozulmaması esasına dayalı olarak fikir geliştirilmiş ve yeni yöntem sunulmuştur.

Name and Surname : Burcu ÜNLÜ
Supervisor : Dr. Lecturer Ediz ŞAYKOL
Type and Year : Master Thesis/2019
Major : Computer Engıneerıng
Keywords : Steganography, Steganography with Alpha Channel

ABSTRACT

STEGANOGRAPHY WITH ALPHA CHANNEL

In this study, it is aimed to introduce a new method to Steganography science methods. Some known methods of Steganography have been examined and techniques have been tried to be explained on current topics. One of the fields of steganography is focused on image and messaging method and it has been shown that Steganography can be performed over alpha channel in some images. The idea was developed on the basis of not distorting the image in the related picture during the sending of confidential messages over the images and a new method was presented.

İÇİNDEKİLER

Sayfa No.

ÜÇÜNCÜ BÖLÜM
ALFA KANALI İLE STEGANOGRAFİ

DÖRDÜNCÜ BÖLÜM
İNCELEME

TABLOLAR LİSTESİ

Sayfa No.

ŞEKİLLER LİSTESİ

Sayfa No.

GİRİŞ

Teknolojinin özellikle 2000'li yılların başından bu yana hızlıca yaygınlaşması ve gelişmesi ile birlikte, günümüzde kurumsallaşmış her bir yapı ve teşkilat açısından veriyi saklama ile veri alışverişi, özellikle hızla artan veri kalabalığı ve güvenlik açıkları nedeniyle ciddi bir mesele haline gelmiştir. Örneğin, devletlerin istihbarat teşkilatları ellerinde bulundurdukları veriyi, bir yandan diğer teşkilatlardan gizlemek için gerekli yöntemleri geliştirmeye çalışırken, diğer yandan veriyi ilgili alıcılara da iletme çabasındadırlar. Bu sebeptendir ki veri gizliliği ve güvenliği, devletin tüm teşkilatlarında önemli bir yer tutmaktadır.

Bu çalışma ile birlikte mesajlaşma verileri üzerinde durularak, tüzel veya gerçek kişiler arasında gerçekleşecek, gizli mesajlaşma yöntem ve biçimlerinden Steganography bilimi tekniklerine yeni bir metot getirilmesi amaçlanmaktadır.

Çalışmanın birinci bölümünde, bilinen gizli mesaj gönderme yöntemleri günümüz örnekleri ile anlatılmaya çalışılacaktır. Bahsedildiği üzere, teknolojinin hızla gelişmeye devam ettiği göz önünde bulundurulduğunda, yöntem ve tekniklerin tamamını tanımlamak mümkün olamayacağı gibi tanımlamaya çalışılacak olanlar için de zaman ve kapsam açısından, en ufak noktalarına kadar derinlemesine analize de yer verilemeyecektir.

Çalışmanın ikinci bölümünde, tez kapsamı ve konusuna ilişkin gizli mesaj gönderme yöntem ve tekniklerinden Steganography bilimi incelenerek, bu bilime ilişkin örnekler ve algoritmalara yer verilmeye çalışılacaktır.

Çalışmanın üçüncü bölümünde Steganography bilimi kapsamında uygulanan gizli veri iletişimine ek, yeni bir yaklaşım ortaya atılacaktır.

Çalışmanın tamamlandığı son bölüm olan dördüncü bölümde ise, yeni bir yaklaşım olarak ortaya atılan tezin, avantaj ve dezavantajları ortaya konulmaya çalışılacaktır.

BİRİNCİ BÖLÜM

MESAJ GİZLEME YÖNTEMLERİ

1. GİZLENMİŞ MESAJ

Mesaj kelimesini, belirlenmiş iletişim kanalları vasıtasıyla taşınan, bir veya birden çok göndericisinin ve alıcısının olduğu bir veri biçimi olarak tanımlamak mümkündür. Örneğin kişilerin ve kurumların telefon, internet, televizyon, radyo, gazete vb. kanallar üzerinden birbirlerine göndermiş oldukları işitsel, görsel ve metinsel veri, mesaj olarak adlandırılabilir.

Mesajın, doğrudan veya dolaylı olarak iletilebileceği gibi şifrelenmiş veya alıcıların tamamı tarafından anlaşılabilir biçimde de gönderilebileceği bilinmektedir. Çeşitli kişi, kurum ve kuruluşlar, mesajın içeriği, gizlilik seviyesi vb. bilgileri kapsamında mesajlarını göndermeden önce şifreleme, maskeleme vb. tekniklere tabii tutarak iletebilmektedirler. Böylelikle mesajlar, şifrelenmiş biçimde alıcılara ulaştırılabilir.

Mesajları şifreleme sonrası gönderme teknikleri günümüzde sıkça kullanılmaktadır. Buna en yaygın örneklerden bir tanesi WhatsApp uygulaması gösterilebilir. Uygulama geliştiricileri ve yetkilileri tarafından söylenen bilgiye göre kişiler arasında gönderilen mesajlar, mesaj gönderilmeden önce şifrelenmekte, mesaj, alıcı tarafından alındıktan sonra ise şifresi çözülerek ilgili kullanıcıya gösterilmektedir. Yine bir diğer örnek olarak HTTPS protokolünden bahsedilebilir. Ziyaret edilen ve HTTPS ile başlayan web sitelerinde yer alan formlara doldurulan bilgilerin sunucuya iletilmesi esnasında şifrelendiği, dolayısıyla 3.kişiler tarafından bilgi aktarımı sırasında araya girilse bile o an için geçerli, çözülmesi mümkün olmayan şifreleme yöntemlerinin kullanıldığı bilinmektedir.

Mesaj şifreleme ile gizleme arasında doğrudan ve dolaylı olarak bir bağ bulunmaktadır. Mesaj gizleme, gönderilecek olan mesajın şifrelenmesinden çok gizlenmesidir. Diğer bir deyişle gizlenmiş mesaj, gönderilen mesaj içerisinde yer alan, yazılı ise gözle görülemeyen, sesli ise anlaşılamayan başka bir mesajdır.

2. MESAJ GİZLEME YÖNTEMLERİ

En tanındık mesaj gizleme yöntemlerinden bir tanesi Mors alfabesi veya Mors kodu ile bilinmektedir. Mors kodu, İngiliz alfabesi ve noktalama işaretlerini kullanacak biçimde Samuel Morse tarafından 1838 tarihinde geliştirilmiş ve kullanılmıştır. [1]

Amerikan elektronik telgraf haberleşmesi için geliştirilmiş Morse kodu, kısa ve uzun işaretler ile ışık veya seslerin birleşimi neticesinde anlamlı gizlenmiş mesaj olarak hemen her alanda kullanılabilmektedir.

Mors kodunun özellikle 1. Dünya Savaşı'nda kullanıldığı bilinmektedir.[2] Dünya Savaşı yıllarında İngiliz ve Amerikan askerlerinin Mors kodunu anlamaları için çeşitli sınıflar kurulduğu da yine arşivler arasında yer almaktadır.[3]

Uluslararası Mors kodu, 26 harf İngiliz alfabesi, rakamlar ve çeşitli noktalama işaretlerinden oluşmaktadır ve tüm Mors kodları, noktalar ve tire (-) işaretlerinden meydana gelmektedirler. Gönderilmek istenen mesaj için nokta ve tire işaretleri arasında çeşitli boşluklar – beklemeler ile uzunluk ilişkisine ilişkin çeşitli kurallar tanımlanmıştır. Bu kurallar:

- 1 tire işareti 3 nokta işaretine eşittir.
- Ardışık gelen harfler arasındaki boşluk 1 nokta
- 2 harf arasındaki boşluk 3 nokta
- 2 kelime arasındaki boşluk 7 nokta

olarak belirtilmiştir. [4]

Örneğin;

```
M   O   R   S  E            C   O   D  E
-- --- .-. ... . (boşluk)   -.-. --- -.. .
```

[1] Massachusetts Institute of Technology, "Samuel Morse", https://lemelson.mit.edu/resources/samuel-morse, 28/04/2019
[2] The National Archives, "Fighting talk: First World War telecommunications", http://www.nationalarchives.gov.uk/first-world-war/telecommunications-in-war/, 28/04/2019
[3] BBC, "WW2 People's War", https://www.bbc.co.uk/history/ww2peopleswar/stories/59/a3890559.shtml, 28/04/2019
[4] International Telecommunications Union, "International Morse code", https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.1677-1-200910-I!!PDF-E.pdf, 28/04/2019

Mors alfabesinin genel biçimini Tablo 1.'de gösterilen biçimde belirtmek mümkündür.

Tablo 1. Mors Alfabesi

Harfler

Harf	Kodu	Harf	Kodu
A	•–	N	–•
B	–•••	O	–––
C	–•–•	P	•––•
D	–••	Q	––•–
E	•	R	•–•
F	••–•	S	•••
G	––•	T	–
H	••••	U	••–
I	••	V	•••–
J	•–––	W	•––
K	–•–	X	–••–
L	•–••	Y	–•––
M	––	Z	––••

Sayılar

Sayı	Kodu
0	–––––
1	•––––
2	••–––
3	•••––
4	••••–
5	•••••
6	–••••
7	––•••
8	–––••
9	––––•

Noktalama işaretleri

İşaret	Kodu	Adı
.	•–•–•–	nokta
,	––••––	virgül
?	••––••	soru işareti
-	–••••–	tire
/	–••–•	taksim

Mors alfabesi İngiliz harflerine dayandığı için ülkelere göre semboller (harfler) değişmektedir. Örneğin Kiril alfabesi için Tablo 2. incelenebilir.

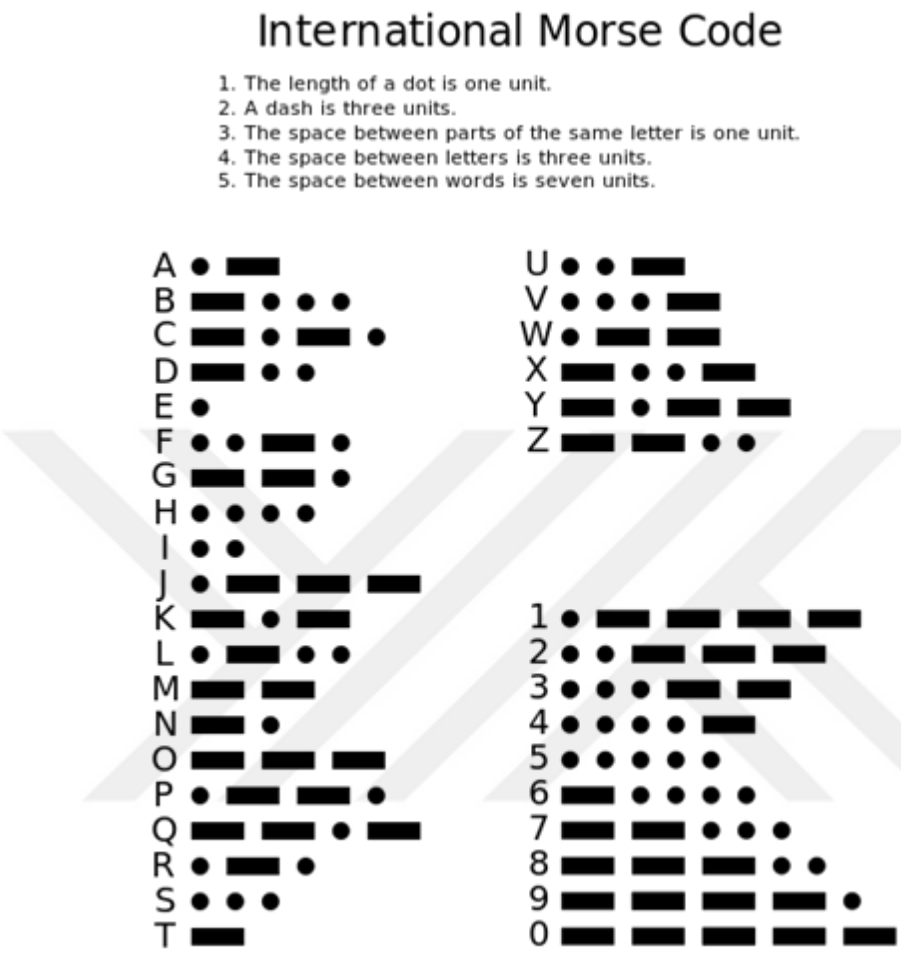
Tablo 2. Kiril Alfabesi için Mors Kodları[5]

Cyrillic	Latin	Code	Cyrillic	Latin	Code	Cyrillic	Latin	Code	Cyrillic	Latin	Code
А	A	▪▬	И	I	▪▪	Р	R	▪▬▪	Ш	CH	▬▬▬▬
Б	B	▬▪▪▪	Й	J	▪▬▬▬	С	S	▪▪▪	Щ	Q	▬▬▪▬
В	W	▪▬▬	К	K	▬▪▬	Т	T	▬	Ь (Ъ)	X	▬▪▪▬
Г	G	▬▬▪	Л	L	▪▬▪▪	У	U	▪▪▬	Ы (Ь)	Y	▬▪▬▬
Д	D	▬▪▪	М	M	▬▬	Ф	F	▪▪▬▪	Э	É	▪▪▬▪▪
Е	E	▪	Н	N	▬▪	Х	H	▪▪▪▪	Ю	Ü	▪▪▬▬
Ж	V	▪▪▪▬	О	O	▬▬▬	Ц	C	▬▪▬▪	Я	Ä	▪▬▪▬
З	Z	▬▬▪▪	П	P	▪▬▬▪	Ч	Ö	▬▬▬▪			

Morse kodunun, ülke alfabelerinde yer alan değişiklikler neticesinde geliştirilmesi ile birlikte günümüzde Tablo 3. deki gibi kullanımları mevcuttur.

[5] Wikizero, "Morse code for non-Latin alphabets", http://www.wikizero.biz/index.php?q=aHR0cHM6Ly9lbi53aWtpcGVkaWEub3JnL3dpa2kvTW9yc2VfY29kZV9mb3Jfbm9uLUxhdGluX2FscGhhYmV0cw, 28/04/2019

Tablo 3. Uluslararası Mors Kodları[6]



[6] University College London, "What is Morse Code?", http://students.cs.ucl.ac.uk/schoolslab/projects/PY2/introduction.html, 28/04/2019

Mors kodu hakkında, geliştirildiği tarihten günümüze bir asırdan fazla zaman geçmesi ve geniş kullanım alanına sahip olması nedeniyle bir çok makale ve bildirim yayınlanmıştır. Yayınlanan eserler incelendiğinde, Mors kodunun, nokta ve tire işaretlerinden oluşan bir dizi simgenin yan yana gelmesi neticesinde ortaya çıkan, sesli ve yazılı olarak kullanılabildiği anlaşılmaktadır. Bu sebeptendir ki; Mors kodu için mesaj gizleme yöntemi diyebilmek ile birlikte Kriptografi bilimi ile de ilişkili olduğunu söylemek mümkün olabilmektir.

Mors kodu dışında, bilinen bazı mesaj gizleme yöntemleri şu şekildedir:

- Görünmez mürekkep[7]
- Mask Letter[8]

Mesaj gizleme yöntemleri, mesaj gizleme tekniklerine uygun olarak geliştirilmişlerdir.

Mesajın gizlenebilmesi için uygulanan teknikler, mesajın saklanacağı objeye fazladan bit veya nesne ekleme, çıkarma veya mesajı saklayacak yeni bir objeyi mesaja göre oluşturma biçiminde gerçekleştirilirler.

[7] University Of Michigan, "Secret methods and Techniques", http://clements.umich.edu/exhibits/online/spies/methods-ink.html, 28/04/2019
[8] University Of Michigan, "Secret methods and Techniques", http://clements.umich.edu/exhibits/online/spies/methods-ink.html, 28/04/2019

İKİNCİ BÖLÜM

STEGANOGRAFİ

1. STEGANOGRAFİ

Steganografi, kökleri Yunanca olan "steganos (gizli, saklı)" ve "graphein (yazı)" kelimelerinin bir araya gelmesi ile "stɛgəˈnɒgrəfi" olarak ortaya çıkmış olan, yazılı bilgiyi gizleme bilimine verilen ad olarak karşımıza çıkmaktadır. Günümüz dünyasında gizlenecek bilgi yalnızca metin olmayacağından dolayı Steganografi bir bilim olarak, metin gizleme sanatından çok daha fazla anlam taşımaktadır.

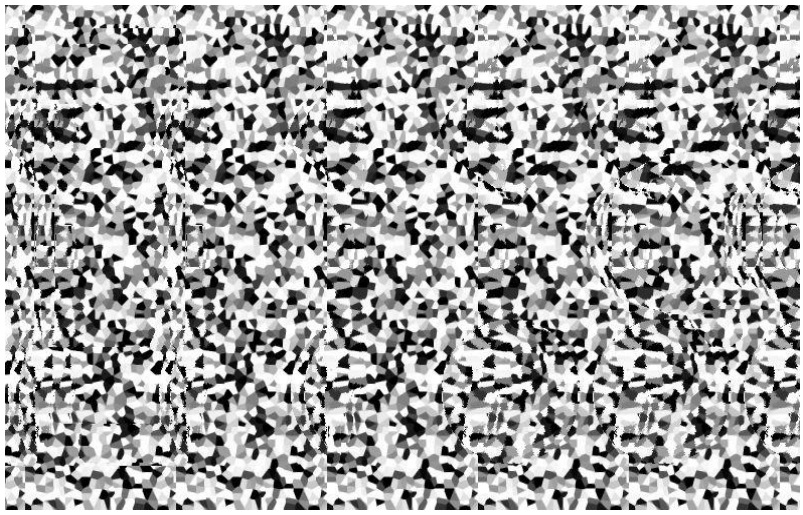
Steganografi biliminde önemli bir amaç, gizlenecek olan bilginin dikkat çekmeyecek biçimde gizlenmesidir. Diğer bir deyişle bilgi, seslerde ise dinlenilen müzikte, resimlerde ise bakılan resimde, videolarda ise izlenilen kayıtlarda, izleyen kişilere bilgi gizlenmesine ilişkin hiçbir his uyandırmayacak biçimde saklanmaktadır. Örneğin, Akrostiş olarak adlandırdığımız şiirler Steganografi bilimi ile alakalı olabilmektedir çünkü okuyucu, şiiri okuduğu zaman başka anlam aramamaktadır. Aynı Cahit Sıtkı Tarancı'nın, Vedia isimli birine yazmış olduğu şiir gibi.

Var olan bir sen, bir ben, bir de bu bahar
Elden ne gelir ki? Güzelsin, gençliğin var
Dünyada aşkımız ölüm gibi mukaddes
İnan ki bir daha geri gelmez bu günler
Âlemde bu andır bize dost esen rüzgar

2000'li yılların başında Eminönü alt geçitlerinde yer alan "Şaşı Bak Şaşır" resimleri de Steganografi bilimi için güzel örnek teşkil etmektedirler. Bu resimlere dikkatlice şaşı bakıp yoğunlaşıldığında içlerinde başka resimler olduğu görülmektedir.

Örnek bir resim **Şekil 1**'de gösterilmiştir.

Şekil 1. Şaşı Bak Şaşır



Steganografi tekniğinin ilk ne zaman ortaya atıldığı bilinmemek ile birlikte konu ile ilgili çok yaygın bir olay anlatılmaktadır.[9] Bahsedilen olaya göre, M.Ö 400'lü yıllarda Sparta kralı Dematrus, Xerces'in Yunanistan'a saldırı planlayacağını bildirmek istemektedir. Saldırı bilgisini saklamak için dikdörtgen bir tabloya saldırı mesajını kazımış ve tahtanın üzerini balmumu ile kaplamıştır. Böylelikle tahtanın, mesajı taşıyan tarafından ve yolda karşılaşabileceği düşman kişiler tarafından, sıradan bir nesne olarak algılanmasını sağlamıştır. Mesajı alan kişi ise balmumunu erittikten sonra altında yazan mesajı görebilmiştir.

Yunan tarihinde Steganografi tekniklerine sıkça rastlamak mümkündür. Bilinen bir diğer örnek, insan vücuduna kazınan mesajı göndermek ile ilgilidir. Mesaj tekniğine göre, mesajı iletecek olan kişinin saçları kazılır, kazılan saçlar sonrasında kafasına, mesaj, dövme veya başka bir biçimde yazılır ve saçlarının uzaması beklenirdi. Saçların uzaması sonrasında mesajı alacak kişiye gönderilir ve yanında saçların tekrar kesilmesi neticesinde mesaj ortaya çıkartılır.

Steganografi biliminin, mesaj gizleme ile ilgili ve M.Ö.'sine dayanan tarihi olduğu düşünüldüğünde, bilim ile ilgili bir çok teknik geliştirildiğini söylemek mümkündür.

[9] Çağdaş DERELİ, **"Dilbilimsel Steganografi Yöntemleri Üzerine Bir Araştırma"**, Ege Üniversitesi, 2010

1.1. Steganografi Teknikleri

Steganografi, birçok alan ve şekilde kullanılabilir. Steganografi teknikleri, insan aklına gelebilecek tüm platform ve durumlarda oluşturulabileceği için, bu tekniklerin tamamını söyleyebilmek mümkün olmamak ile birlikte, aşağıda bazı örnekler verilmiştir.

- Görüntü dosyalarına ait piksellerin değiştirilmesi
- Videolara gizli mesajlar ve resimler saklama
- Şarkıların tersten çalınması ile mesajı saklama
- İnsan mimikleri
- Yazılan mektuplar, çekilen fakslar gibi metinsel mesaj gönderimlerinde yer alan cümlelerde gizlenmiş mesajlar
- Akrostiş şiirler
- İnsan vücuduna çizilen dövmelerde yer alan gizli mesajlar

gibi akla gelebilecek her türden mesaj gizleme yöntemlerinin tamamı Steganografi tekniklerini oluşturmaktadır.

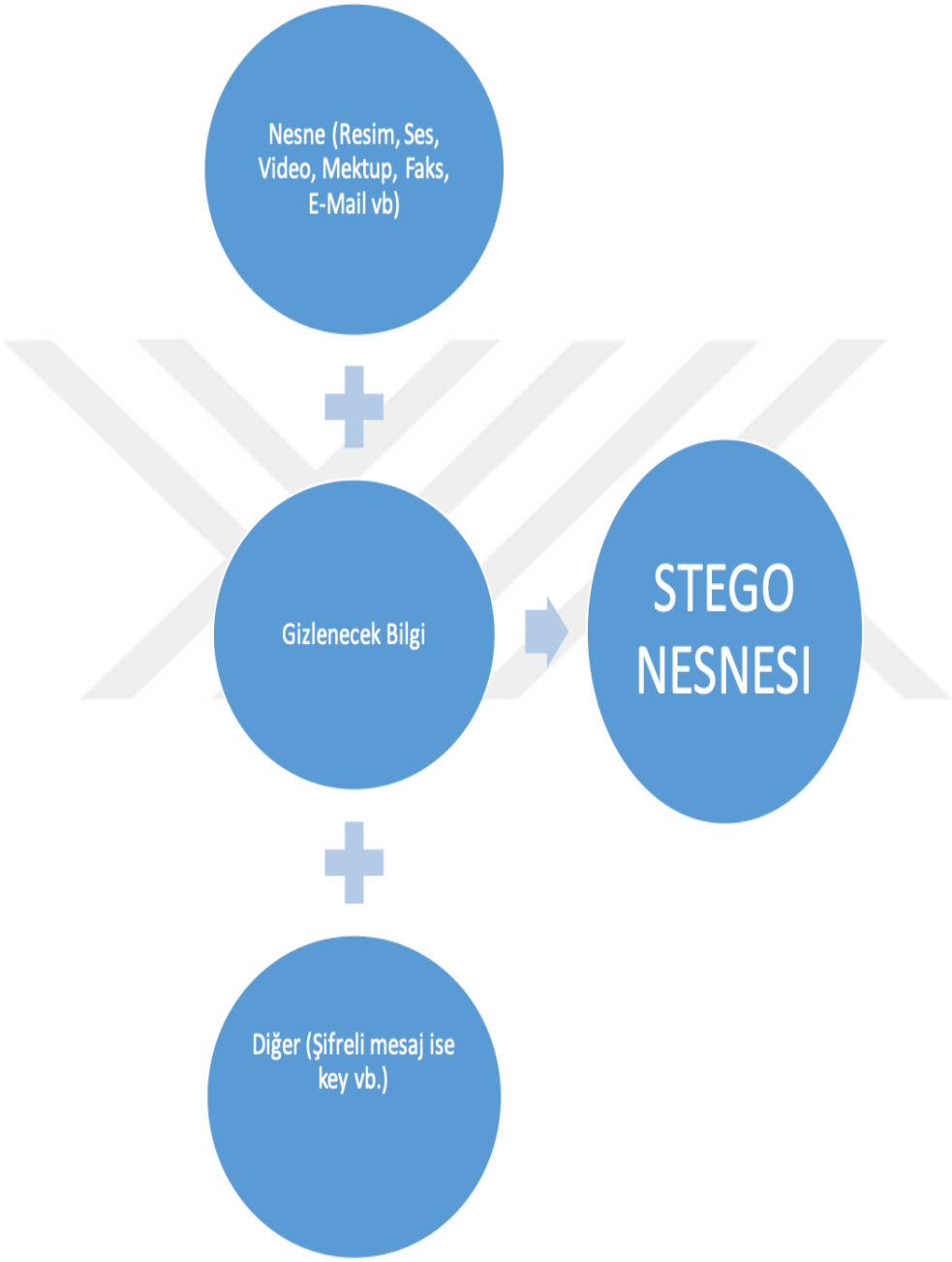
Steganografi tekniklerini insan duyuları ile gruplamak da mümkün olabilir.

- Görsel teknikler (video, görüntü vb. içerisine gizlenmiş mesajlar)
- İşitsel teknikler (şarkılar, konuşmalar vb. içerisine gizlenmiş mesajlar)
- Dokunsal teknikler (örneğin engelli vatandaşlar için geliştirilen klavye vb.)
- Koku almaya yönelik geliştirilen teknikler (örneğin sıkılan parfüme göre önceden belirlenmiş mesajlar)
- Tat almaya yönelik geliştirilen teknikler (örneğin yemeğin içine koyulacak baharata göre önceden belirlenmiş mesajlar)

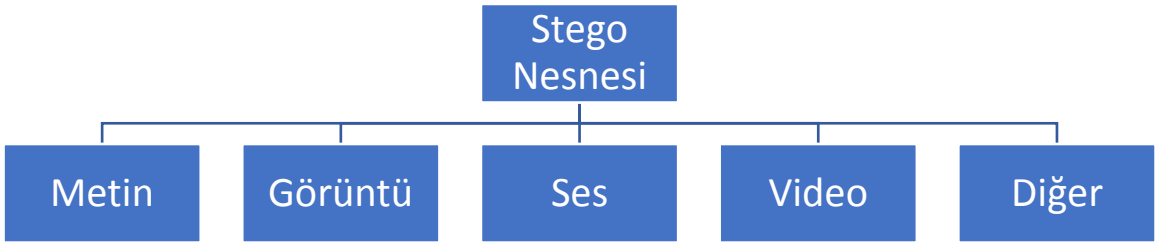
Steganografi tekniklerinin, gelişen teknoloji ve teknolojinin yaygın kullanılması neticesinde özellikle dijital dünyada pek çok örneği mevcuttur.

Steganografi ile gönderilmek istenen mesajlar, şifrelenmiş veya açık biçimde de gönderilebilir. Mesajın son hali ile mesajın gizleneceği nesnenin birleşimi sonucu gönderilen nesne **Stego** nesnesi olarak adlandırılmaktadır.

Şekil 2. Stego Nesnesi



Steganografi teknikleri, stego nesne tiplerine göre de ayrılmaktadırlar.



1.1.1. Metinsel Steganografi

Metinsel Steganografi, metin içerisinde metin saklama demektir. [10] Bu teknik, mektup, e-mail, faks, gazete, dergi vb. tüm metinsel içeriklere uygulanabilir.

Metinsel Steganografi teknikleri günümüzde yaygın olarak aşağıdaki gibi kullanılmaktadır:

- Yazının her n. harflerinden elde edilen gizli metin
- Kelimeler arasında yer alan boşluk sayısı

1.1.2. Ses ile Steganografi

Ses ile Steganografi, gizlenecek olan mesajı dijital ses dosyaları üzerinde saklama tekniğidir. Örneğin bazı şarkıların, sondan başa doğru sarıldığında başka sözcükler içeren şarkı oldukları görülebilir. [11]

[10] Neha Rani ve Jyoti Chaudhary, "Text Steganography Techniques: A Review", http://www.ijettjournal.org/volume-4/issue-7/IJETT-V4I7P186.pdf, 28/04/2019
[11] Anonim, "Juntin Bieber Baby (Reversed)", https://www.youtube.com/watch?v=vgphZB5lzT0, 28/04/2019

Ses ile Steganografi teknikleri, yaygın olarak, ses dosyası üzerinde aşağıdaki özel teknikler ile oluşturulurlar.

- Low bit encoding
- Spread Spectrum
- Echo data hiding

1.1.3. Video ile Steganografi

Video ile Steganografi teknikleri ile dijital video içerisine ses, görüntü ve metin yerleştirilebilmektedir. Bu duruma genellikle televizyon yayın ve reklamlarında rastlanılmaktadır. [12]

Video ile Steganografi tekniği yaygın olarak DCT (Discrete Cosine Transform) yöntemi ile oluşturulmaktadır.

1.1.4. Görüntü ile Steganografi

Steganografi tekniklerinden en yaygın olanı, dijital görüntü işleme teknikleri ile gerçekleştirilen görüntü ile Steganografi tekniğidir. Bu alanda geliştirilen teknikler ile resim içerisine başka bir resim veya metinsel mesajlar yazılabilmektedir.

Görüntü ile Steganografi tekniğinde genel yaklaşım, resim piksel değerlerinin değiştirilmesi suretiyle mesaj veya başka bir resim saklama çalışmasıdır.

Görüntü ile Steganografi teknikleri ile bilgi gizlemede en çok bilinen yöntemler aşağıda verilmiştir.

- En önemsiz bite ekleme
- Maskeleme ve Filtreleme

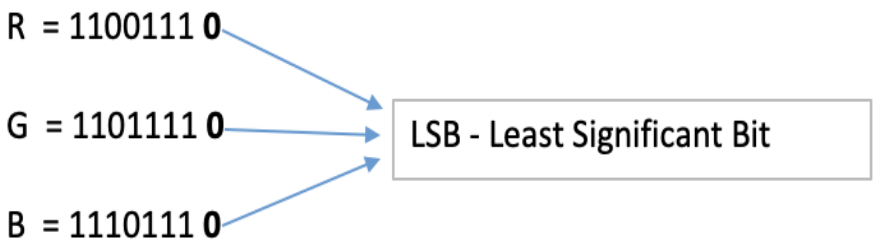
[12] Cambridge Üniversitesi, "Digital Watermarking", https://www.cl.cam.ac.uk/teaching/0910/R08/work/essay-ma485-watermarking.pdf, 28/04/2019

1.2. En Önemsiz Bite Ekleme (LSB – Least Significant Bit)

Bilindiği üzere resmin her bir pikseli, kırmızı, yeşil ve mavi renklerinin karışımından oluşmaktadır. Bu karışıma esas olan renklerin oluşturduğu uzay, RGB Renk Uzayı olarak adlandırılmaktadır. Her bir renk 8 bit olacak biçimde, [0-255] yani bit gösterimi olarak, 00000000 – 11111111 aralığında değer almaktadır.

LSB Steganografi tekniği ile gönderilecek olan mesaj, resmin ilgili piksellerinde yer alan RGB (Red – Green – Blue) değerlerinin son bitlerinde saklanılmaktadır. Mesajın ve kullanılan şifrenin durumuna göre son bit gerçek değeri, 1 ise 0, 0 ise 1 olarak yer değiştirebilir veya aynı kalabilir.

Şekil 3. En Önemsiz Bit



Piksel renginin oluşumunu sağlayan RGB değerlerinin her birinin son bitinde yer alan 1 veya 0 değerinin en önemsiz bit olarak adlandırılmasının nedeni, ilgili renk değerini 1 veya 0 olarak arttırıp azaltmasıdır ki bu da gözle görülemeyecek bir değişim demektir. Diğer bir değişle, kırmızı renk için 255 değerini kullanmak ile 254 değerini kullanmak arasında gözle görülebilir bir fark oluşmamaktadır.

LSB tekniği için seçilen son bit dışındaki diğer bitler sırasıyla 2^1, 2^2,…., 2^7 değerlerini temsil ettikleri için bu bitlerde yer alan değişim, resimde anlamlı bir değişikliğe yol açabilecektir.

LSB teknikleri uygulanan görüntü formatları veri kayıpsız sıkıştırma yöntemleri içeren formatlar olmak durumundadırlar. Örneğin Jpeg formatlı resimlerde, pikseller belirli değişikliklere uğratıldıktan sonra hafıza üzerine kaydedilmektedirler. Bu durum, saklanan mesajın bozulmasına ve veri kayıplarına yol açabilmektedir.

LSB teknikleri uygulanan resim formatı, hafızaya kaydedildikten sonra veri kayıplarına uğramayacak biçimde olmalıdır. Bu sebeple PNG veya BMP formatlı resimler iyi bir tercih olacaktır.

Tekniğin uygulanacağı resim boyutu da önemlidir. 1024 x 1024 boyutlu bir resimde 1,048,576 piksel ve buna bağlı olarak 1,048,576 x 3 = 3,145,728 tercih yapılabilmektedir. Gizli mesajın her bir harfi 1 byte olacak biçimde bir algoritma geliştirildiğinde bu resim için LSB tekniği uygulanmak istenildiğinde 3,145,728 / 8 = 393216 kelimelik bir mesaj iletimi mümkün olabilmektedir.

Bir örnek olarak bir resmin örnek kesitinden alınan 3 x 3 kesit piksel değerleri şu şekilde olsun:

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

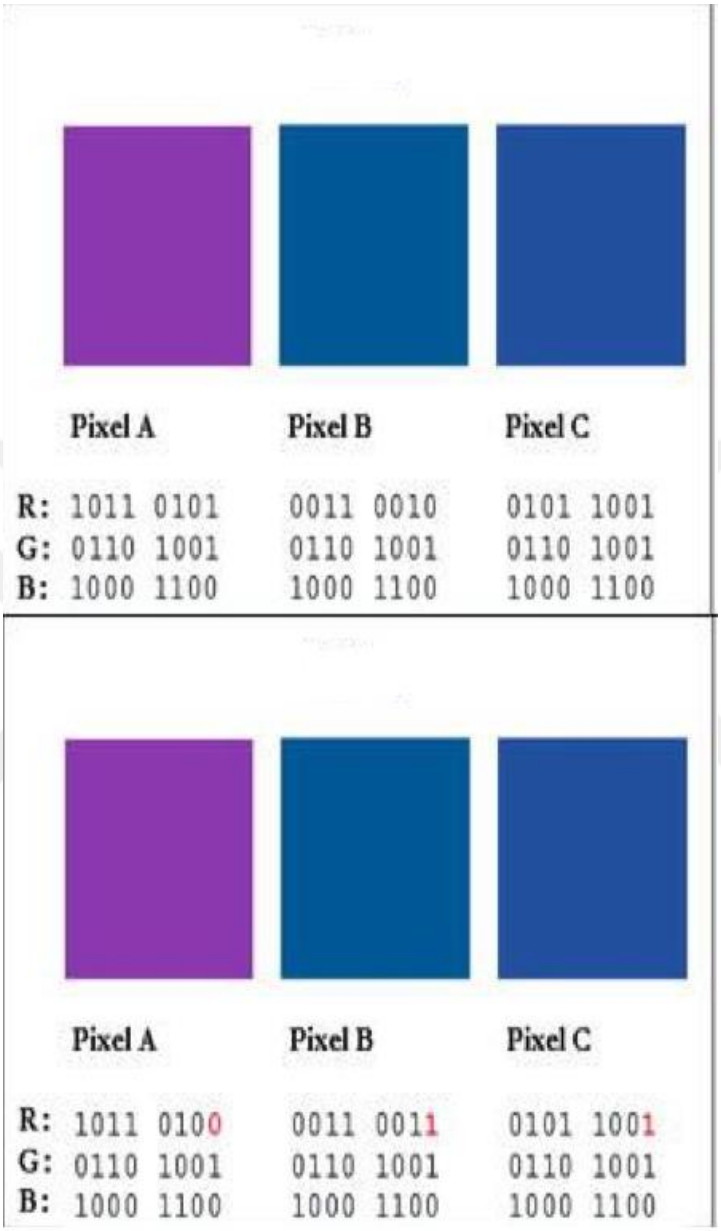
A harfi 10000011 ile temsil edilmek istenildiğinde, resim piksellerinde oluşacak değişim için:

(00100111 1110100<u>0</u> 11001000)
(0010011<u>0</u> 11001000 1110100<u>0</u>)
(11001000 00100111 11101001)

şeklinde olacağı söylenebilir. Bu durumda, A harfini saklayabilmek için 3 adet renk değişiminden bahsedilebilmekle birlikte bu değişim, her bir renk için 1 bit olacağından insan gözü ile fark edilemez.

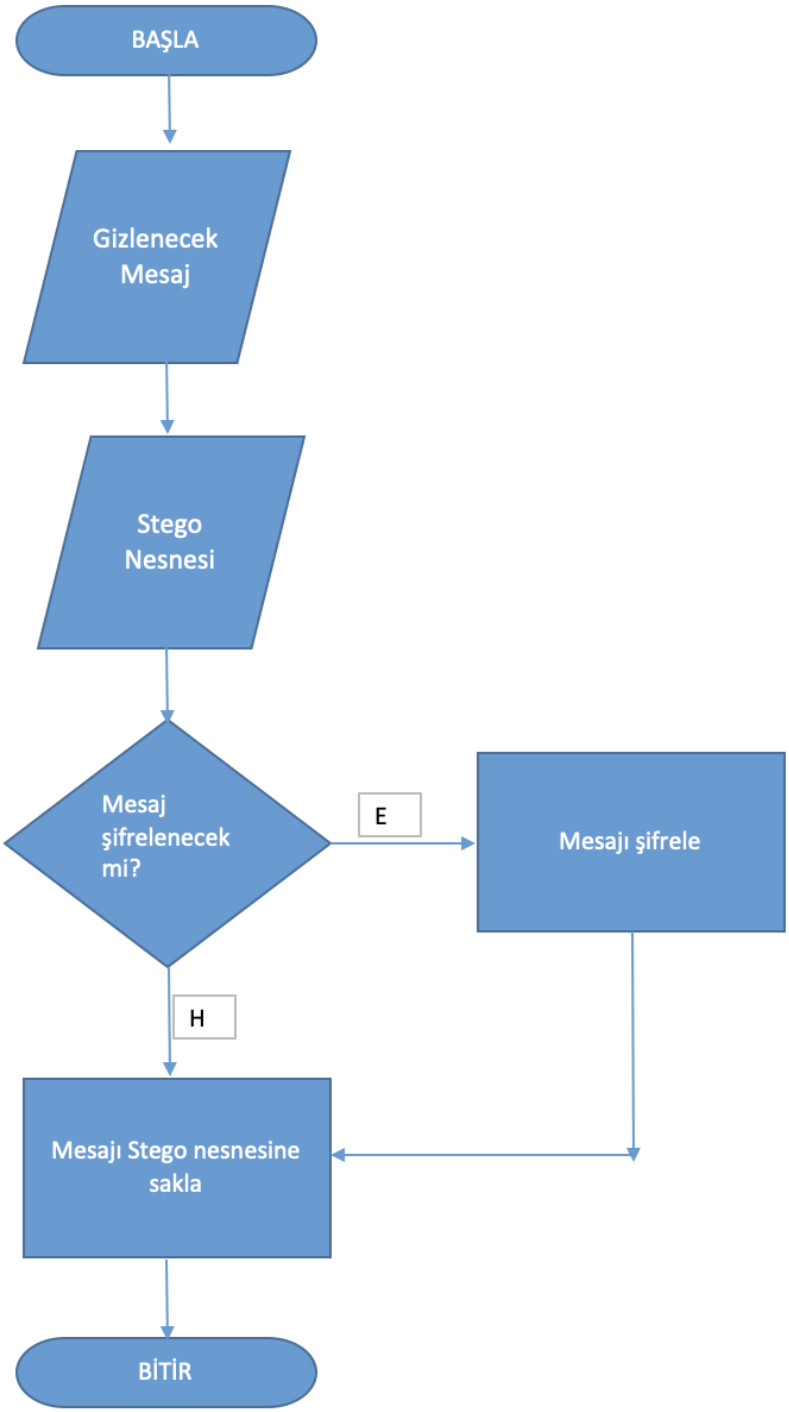
Şekil 4. üzerinde LSB tekniği uygulanmış farklı bir görüntü verilmiştir. Bu görüntüde renkleri insan gözü ile ayırmak mümkün olmamaktadır.

Şekil 4. LSB Tekniği



Her bir Steganografi yöntemi kendine has bir algoritma içermektedir. Steganografi tekniklerine ilişkin genel yaklaşım **Şekil 5** ile gösterilmiştir.

Şekil 5. Steganografi Genel Yaklaşım Algoritması



1.3. Maskeleme ve Filtreleme

Maskeleme ve filtreleme, görüntüye rahatsızlık vermeyecek biçimde, dikkatlice bakıldığında şeffaf olarak yerleştirilmiş yazı ekleme tekniğidir. Bu teknik, günümüzde daha çok Digital Watermarking olarak adlandırılan, görüntüye genellikle, görüntü sahibini ve telif haklarını içeren mesajlar saklayan yapıya benzemektedir. Maskeleme ve Filtreleme ile Digital Watermarking arasındaki fark, kullanım amaçlarıdır. Digital Watermarking'de görüntü içerisine yerleştirilen mesaj görüntüye ilişkin bilgileri içermeyi hedeflemekte iken Maskeleme ve Filtreleme tekniğinde görüntü ile alakasız başka bir mesaj veya görüntü ile ilişkilendirilmeye çalışılmaktadır.

Şekil 6. Maskeleme ve Filtreleme

Steganografi teknikleri ile kullanılan yöntemlerde gizlenecek mesaj, ilgili teknik kullanılmadan önce de şifrelenerek saklanabilir. Bu durumda mesaj gizliliği ve güvenlik seviyesi arttırılmış olunur. Burada şifreleme ile Kriptografi tekniklerinden bahsedilmek istenilmektedir.

2. KRİPTOGRAFİ

Kriptografi, şifreleme bilimi olarak adlandırılmaktadır. Bir veri veya veri seti üzerinde gerçekleştirilen şifreleme çalışmalarının tamamı Kriptografi bilimi içerisine girmektedir.

Kriptografi, veri şifreleme tekniklerini ele aldığından, veri gizliliği esas olan kurumlar için hayati öneme sahip bir kavramdır. Örneğin, kullanıcı adı ve şifre ile giriş yapılan tüm sitelerde, kullanıcı sisteme giriş bilgilerinin çalınması ihtimaline karşı, kullanıcı şifreleri, ilgili veritabanlarına ait tablolarda şifrelenmiş biçimde tutulmalıdırlar. Böylelikle belirli Kriptografi teknikleri ile tutulan şifreler, bilgiler çalınsa dahi uzunca bir müddet deşifre edilemeyebilirler.

Kriptografinin günümüzde yaygın ve kullanılan bir çok tekniği bulunmaktadır. En yaygın Kriptografi teknikleri:

- Simetrik Şifreleme Algoritmaları
    - DES (Data Encrytion Standard - Veri Şifreleme Standartı)
    - AES (Advanced Encrytion Standard - Gelişmiş Şifreleme Standartı)
    - Blowfish
    - IDEA
    - CAST-128

- Asimetrik Şifreleme Algoritmaları
    - DH (Diffie-Helman)
    - RSA (Rivest-Shamir-Adleman)
    - DSA
    - Ed448
    - Elliptic curve

- Anahtarsız Algoritmalar

Kriptografi ile Steganografi bilimleri arasında doğrudan bağ olabilmektedir. Steganografi bilimi teknikleri ile gönderilmek istenen mesaj Kriptografi bilimi teknikleri ile şifrelendikten sonra alıcısına iletilebilir. Bu durum Şekil 7. ile gösterilmeye çalışılmıştır.

Şekil 7. Kriptografi ve Steganografi

ÜÇÜNCÜ BÖLÜM

ALFA KANALI İLE STEGANOGRAFİ

1. RGB RENK UZAYI

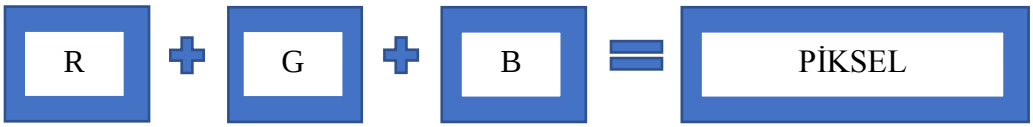
Doğada bulunan, insan gözü ile görülebilen, siyah ve beyaz dışındaki her renk, kırmızı, sarı ve mavi renklerinin çeşitli tonlarda bir araya gelerek karıştırılması ile oluşurlar. Beyaz ve siyah renkler ise, cismin güneş ışığına gösterdiği tepki sonucu ortaya çıkar. Bir cisim güneşten gelen ışınları yansıtmıyorsa siyah, tümünü yansıtıyorsa beyaz rengi alır. Herhangi bir renge siyah eklendiğinde o rengin koyu tonu, beyaz eklendiğinde ise rengin açık tonu elde edilmektedir.

Dijital dünyada ise Güneş sistemi yer almadığından renkleri oluşturmak için farklı algoritmalar ve yaklaşımlar geliştirilmiştir.

Dijital resimler, piksel adı verilen, rengin kendisini temsil eden parçaların birleşiminden oluşur. Her pikselde yer alan renkler, kırmızı, yeşil ve mavi renk tonlarının karışımı sonucu ortaya çıkar.

Şekil 8. Renk Karışımları

Kırmızı, yeşil ve mavi renk tonlarının oluşturduğu karışım, RGB Renk Uzayı olarak adlandırılır. Burada R harfi kırmızıyı, G harfi yeşili ve B harfi ise mavi rengi temsil eder. Her bir renk, hafızada 8 bitlik bir yer kaplar. 8 biti onluk sistemde [0-255] aralığındaki sayma sayıları ile belirtmek mümkündür.



1.1. Alfa Kanalı

Alfa kanalı, resimlerde yer alan piksellerin her birinin, ne kadar şeffaf olduklarını göstermek için kullanılan RGB dışındaki diğer kanaldır. Böylelikle bu tür resimlerde uzay, ARGB olarak adlandırılmaktadır. Alfa kanalı hafızada 8 bitlik bir yer kaplar ve bu durumdaki resimler için her bir piksel 32 bit (A + R + G + B) yer tutmaktadır.

Alfa kanalı ile piksel rengi arasında bir ilişki yoktur çünkü piksel bahsedildiği üzere, kırmızı, yeşil ve mavi renklerinin çeşitli tonları ile oluşur. Öte yandan bu kanal, orijinal resmin, resmin bulunduğu arka plana göre ne kadar gözükeceği ile ilgilidir. Orijinal resmin ilgili pikselinde yer alan alfa değeri 0 ise bu, o pikselin ön planda gözükmeyeceği, 255 ise ilgili pikselin ön planda gözükeceği anlamına gelmektedir. Bu durum literatürde, şeffaflık (transparency) veya şeffaf olmayan (opacity) olarak adlandırılır.

Alfa kanalı, Şekil 9 da gösterilen basit bir html kodu ile anlatılmaya çalışılırsa;

Şekil 9. Html Kod

```
<html>
<head>
<style>
body  {
  background-image: url("black.png");
  background-color: #cccccc;
}
img {
  opacity: 1;
}
</style>
</head>
<body>
    <div id=imagediv>
    <img src="white.jpeg" alt="beyaz">
    </div>
</body>
</html>
```

Şekil 9 ile basit bir web sayfası oluşturulmuş, arka plan resmi için yalnızca siyah renkten oluşan bir resim ve gövde kısmına ise beyaz bir resim bırakılmıştır. Böylelikle arka plan bir resim ve gövdenin de başka bir resim olması neticesinde, iki resim üst üste sayfaya yerleştirilmiştir.

Şekil 9 ile oluşturulan web sayfasında opacity değerleri 1, 0.5 ve 0 olarak değiştirilerek önyüze gelen çıktı incelenmiştir. Burada opacity kelimesi şeffaflık kelimesinin zıttı olan opaklık değeri içindir. Dolayısıyla opaklık ile şeffaflık arasında ters orantılı bir ilişki bulunmaktadır.

Şekil 9'da yer alan opacity değeri sırasıyla 1, 0.5 ve 0 olarak verildiğinde, html çıktısı olarak aşağıdaki durumlar elde edilir.

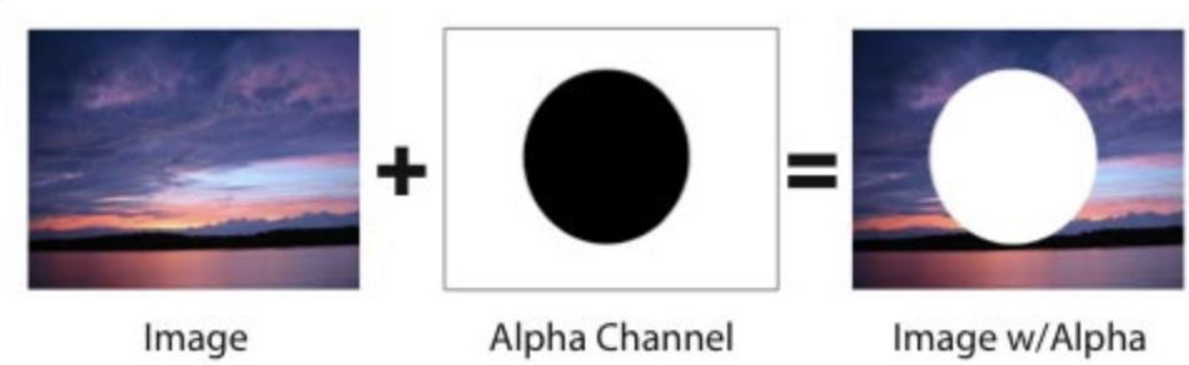
Şekil 10. Opacity = 1 (%100 transparan)

Şekil 11. Opacity = 0.5 (%50 transparan)

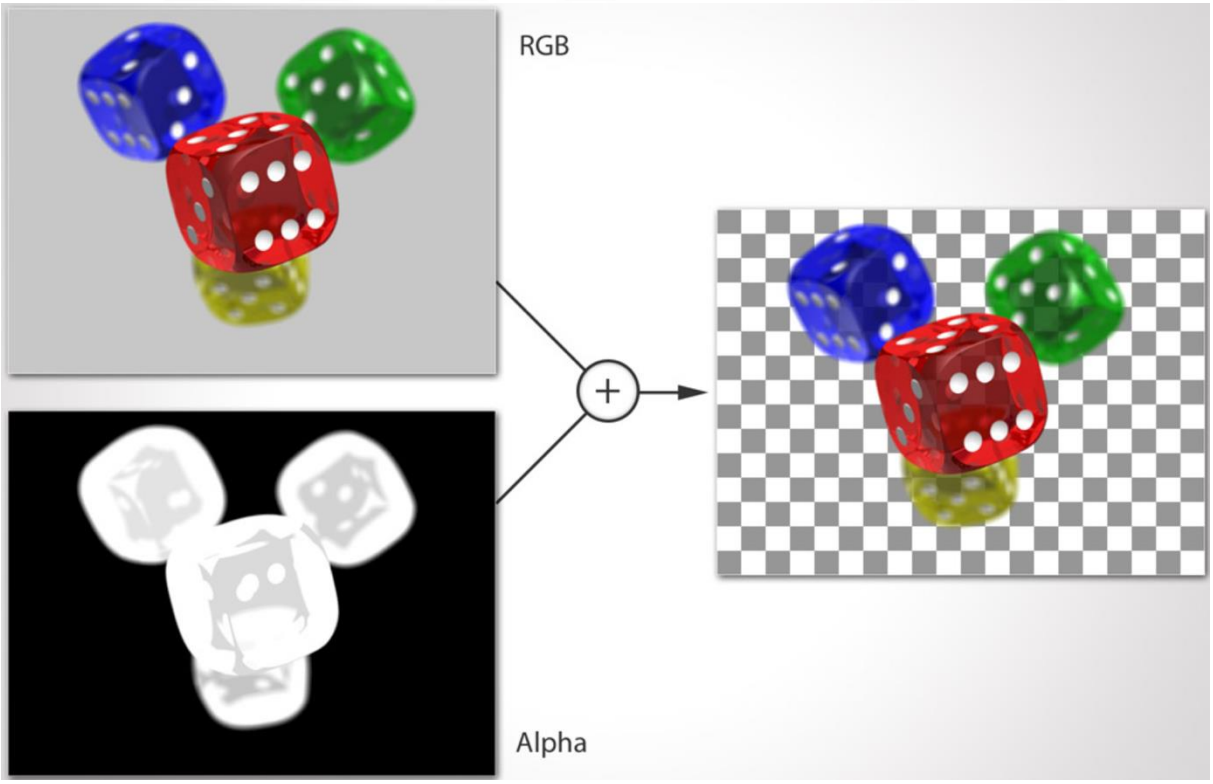
Şekil 12. Opacity = 0 (%0 transparan)

Alfa kanal değerinin de, iki resmin üst üste gelmesi ile benzer bir biçimde bir zemin ve zemin üzerinde yer alan gerçek resmin, şeffaflık değerleri ile ne kadar ön plana çıkacağını belirtmek için kullanılan kanal olduğu aşağıdaki şekiller ile de gösterilmeye çalışılmıştır.

Şekil 13. Alfa Kanalı Örnek 1



Şekil 14. Alfa Kanalı Örnek 2



2. ALFA KANALI İLE STEGANOGRAFİ

Alfa kanalı, resmin şeffaflığı ile ilgili olduğundan, kanal üzerinde yapılacak çeşitli değişiklikler ile resmin görünüşünde değişiklik yapmadan ilgili kanal üzerinde gizli veri taşımak mümkündür.

Bu zamana kadar yapılan çalışmalar araştırıldığında, Alfa kanalı ile RGB değerlerini bir arada kullanmak suretiyle resim içerisinde gizlenmiş başka bir resim gönderilebildiği de ortaya atılabilmiştir.[13]

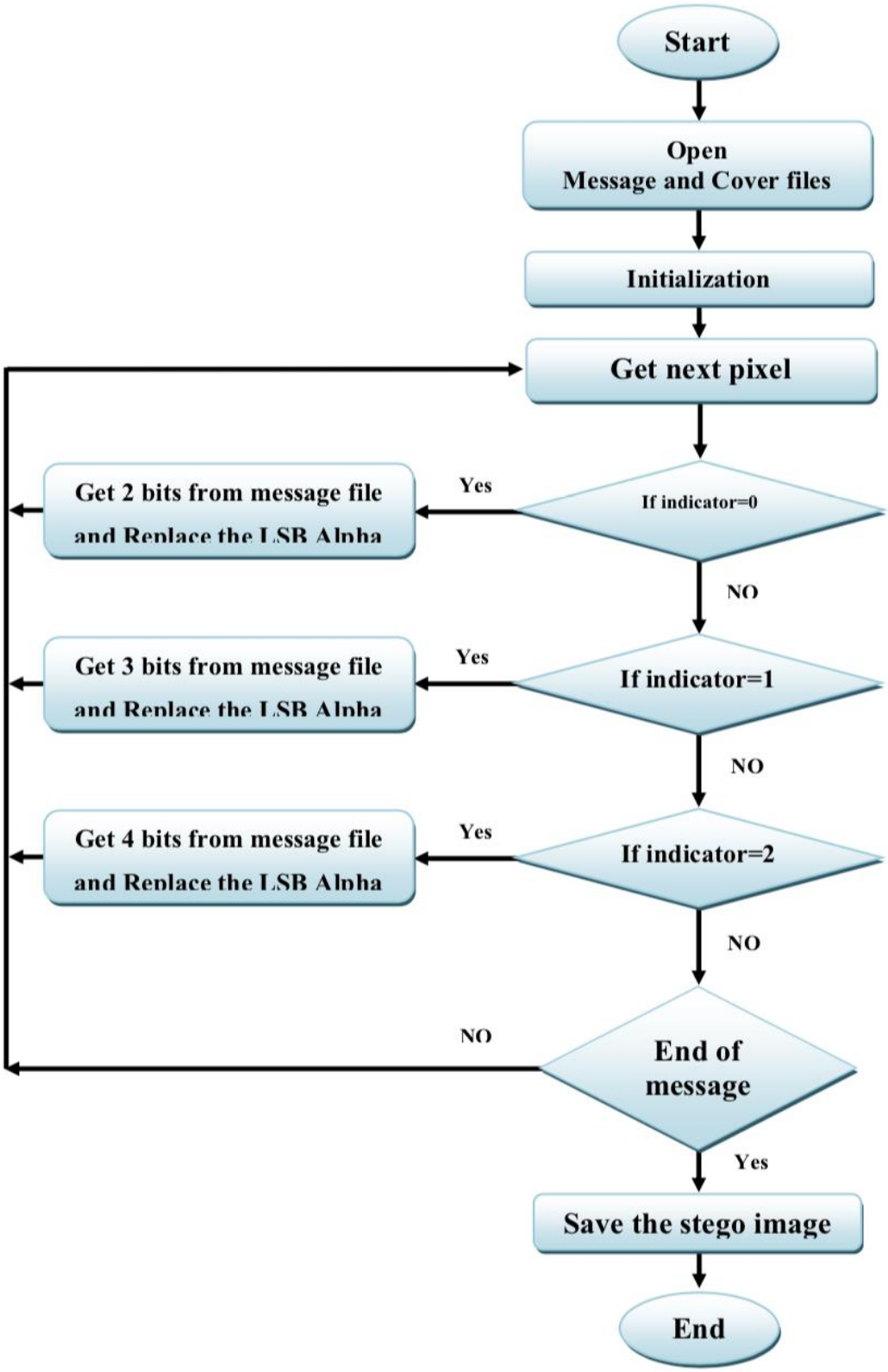
Alfa kanalı ile resim içerisinde resim gönderilen teze ilişkin yapılan çalışma, resmin RGB değerleri ve Alfa kanalı kombinasyonundan oluşmaktadır. RGB değerleri, Alfa kanalında saklanacak bitlerin seçiminde kullanılmaktadır. Buna yaklaşıma göre bahsi geçen tezde alfa değerleri hiç değişmeden taşınabilmekte ve deşifre edilebilmesi için de yine orjinal resim dosyası gerekmektedir. Yaklaşıma ilişkin algoritma Şekil 15 te verilmiştir.

Alfa kanalı ile yapılan bir diğer çalışmada yine resim içerisinde resim gönderme örneğine rastlamak mümkündür. [14]

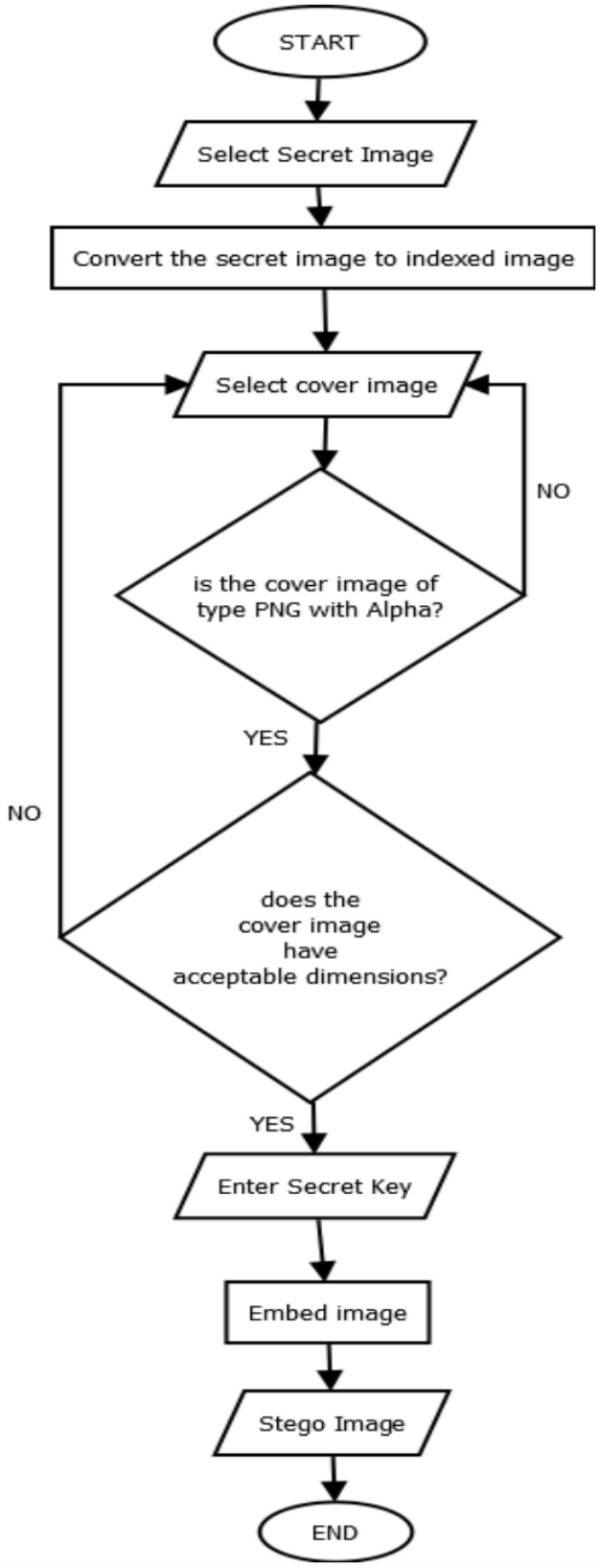
Bu yeni yaklaşıma göre, saklanacak olan resmin saklanmadan önce, boyutu küçültülmektedir. Boyut küçültme işlemi, Lempel-Ziv-Welch (LZW) tekniği ile yapılmakta, ardından resmin belirli bitleri XOR işlemine tabii tutulduktan sonra saklama işlemine geçilmektedir. Yaklaşıma ilişkin algoritma Şekil 16 da verilmiştir.

[13] Ghaith Salem Sarayreh, **"Text Hiding in RGBA Images Using the Alpha Channel and the Indicator Method"**, Middle East University, 2014
[14] Ahmed Faleh, **"New Method for Image Inside Image Steganography"**, Middle East University, 2014

Şekil 15. "Text Hiding in RGBA Images Using the Alpha Channel and the Indicator Method" Tez Algoritması



Şekil 16. "New Method for Image Inside Image Steganography" Tez Algoritması



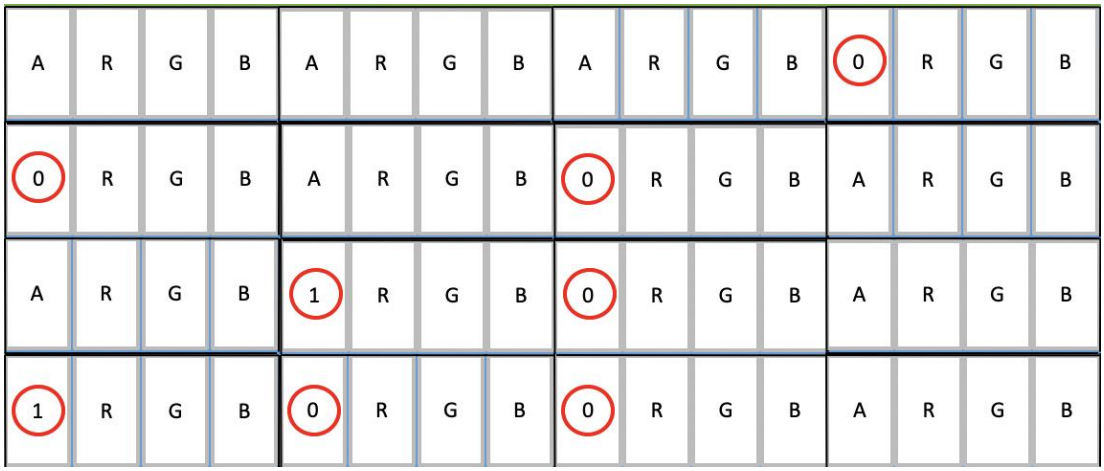
Bu çalışma ile, yalnızca Alfa kanalı kullanılması ve şeffaflık dahil resim piksellerinde gözle görülebilir herhangi bir değişiklik yaşanmadan metinsel mesaj gönderimine ilişkin yeni bir teknik ortaya atılmıştır.

2.1. Tezin konusu olan yaklaşım

Yalnızca Alfa kanalının kullanılmasına ilişkin olan bu teknik genel hatlarıyla aşağıdaki adımları içermektedir.

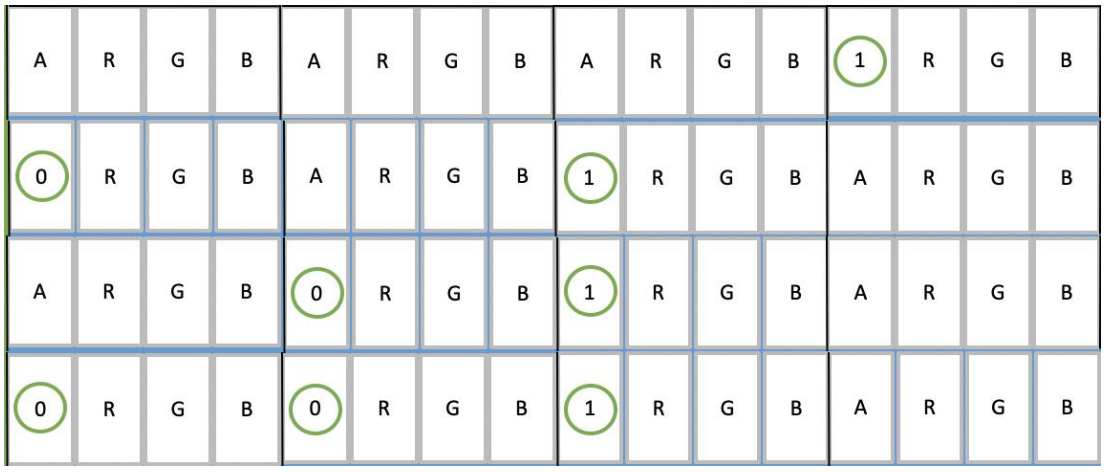
- Resim piksellerinde yer alan, yalnızca 0 veya 1 değerli alfa değerleri kullanılır.
- Gönderilmek istenen mesaj için, her bir harf 8 bit olacak biçimde haritalama yapılır.
- Resim pikselleri, yukarıdan aşağıya (y ekseni) doğru taranır ve 0 veya 1 alfa değeri taşıyan piksele gelindiğinde, mesaja ait sıradaki harfe ilişkin bit 0 veya 1 olarak ilgili pikselin alfa değerine yazılır.
- Mesajın bittiğine ilişkin belirlenen işarete ulaşıldığında taramaya son verilir.

Şekil 17. Örnek orijinal resim pikselleri



Şekil 17'da belirtilen piksellere ilişkin ve değerleri 0 veya 1 olan alfa kanalları kırmızı ile işaretlenmiştir. Gizlenmek istenen mesaj işaretlenen noktalara yerleştirilir. Örneğin M harfinin haritalanmış değeri 00001111 olsun. Bu durumda yeni görüntü **Şekil 18**'deki gibi olacaktır.

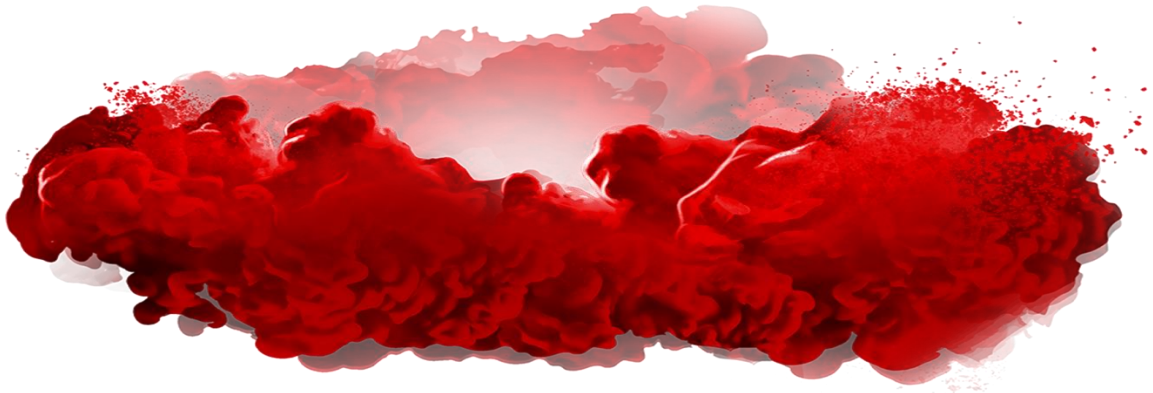
Şekil 18. Örnek orijinal resimdeki değiştirilen pikseller



Alfa kanalında meydana gelen bu değişime ilişkin örnek **Şekil 19** ve **Şekil 20** de gösterilmiştir.

Şekil 19. Örnek orijinal resim

Şekil 20. Örnek orijinal resim değişikliği



2.2. Saklama Algoritması

Adım 1:

Başla

Adım 2:

Saklanacak metni al

Adım 3:

Metnin saklanacağı nesneyi al

Adım 4:

Nesne üzerinde, (metin * 8)+8 den fazla 0 veya 1 değeri içeren alfa kanalı var ise Adım 5'e git, yok ise Adım 10'a git

Adım 5:

Metni, 0 veya 1 olacak biçimde bitsel duruma dönüştür.

Adım 6:

Metnin bitsel biçiminin sonuna 11111111 değerini ekle

Adım 7:

Resim piksellerini okumaya başla.

Adım 8:

Piksel alfa kanalı değeri 0 veya 1 ise metin dizisindeki sıradaki bit değerini piksel alfa değerine ata, değilse bir sonraki pikseli oku.

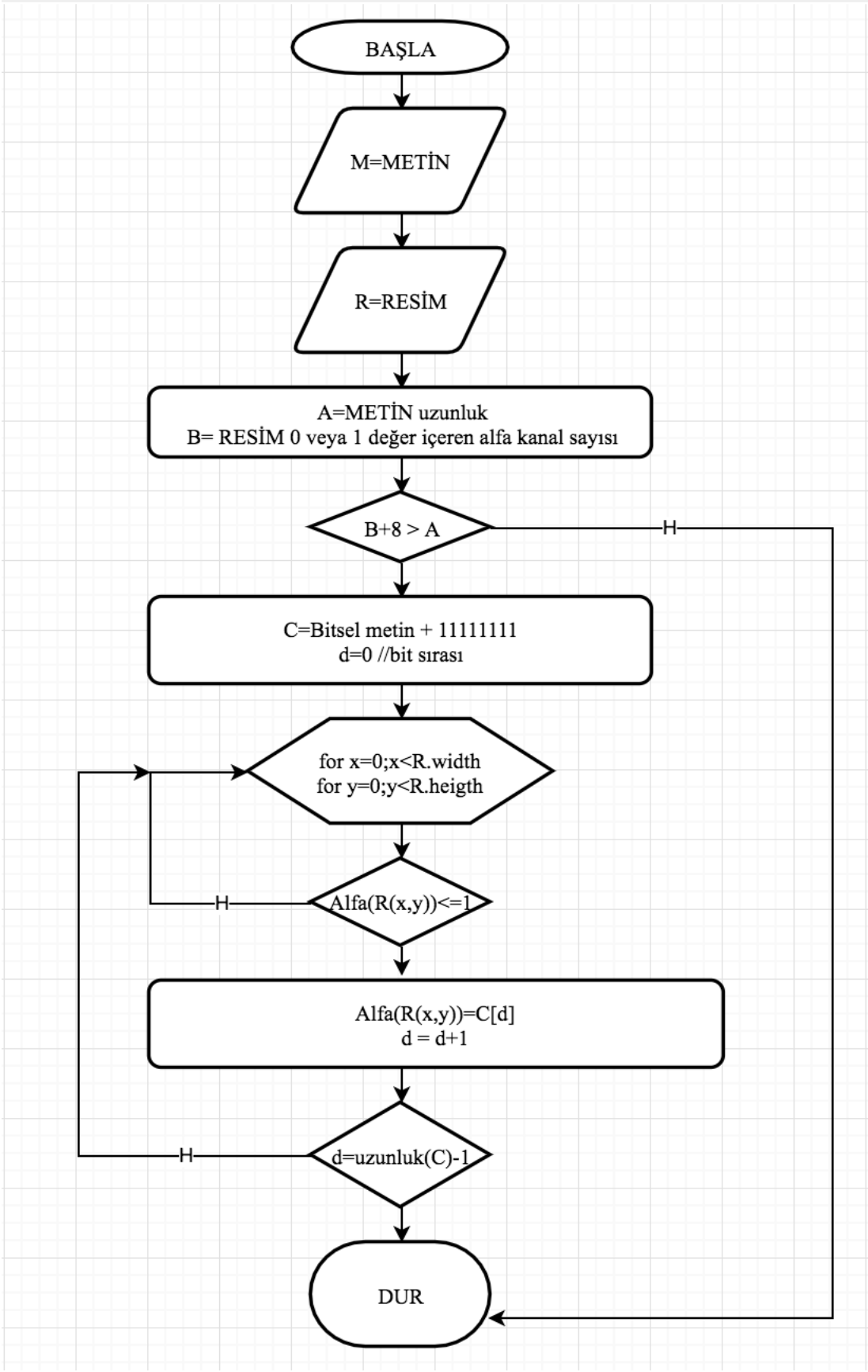
Adım 9:

Metinde okunacak bit kalmamış ise Adım 10'a git, değilse bir sonraki pikseli oku ve Adım 8'e git

Adım 10:

Dur

Şekil 21. Saklama Algoritması



2.3. Çözme Algoritması

Adım 1:

Başla

Adım 2:

Stego nesnesini Al

Adım 3:

Mesaj=””

Bitiş Sayacı=0

Adım 4:

Stego nesnesi piksellerini okumaya başla.

Adım 5:

Piksel alfa kanalı değeri 0 veya 1 ise Mesaj değişkeninin sonuna ekle

Adım 6:

Piksel alfa kanalı değeri 1 ise Bitiş Sayacı değerini 1 arttır, değilse Bitiş Sayacı değerini 0 olarak işaretle

Adım 7:

Bitiş Sayacı değeri 8 ise Adım 8’e değilse bir sonraki pikseli oku ve Adım 5’e git

Adım 8:

Mesajın son 8 karakterini sil

Adım 9:

Mesajı metinsel gösterime çevir

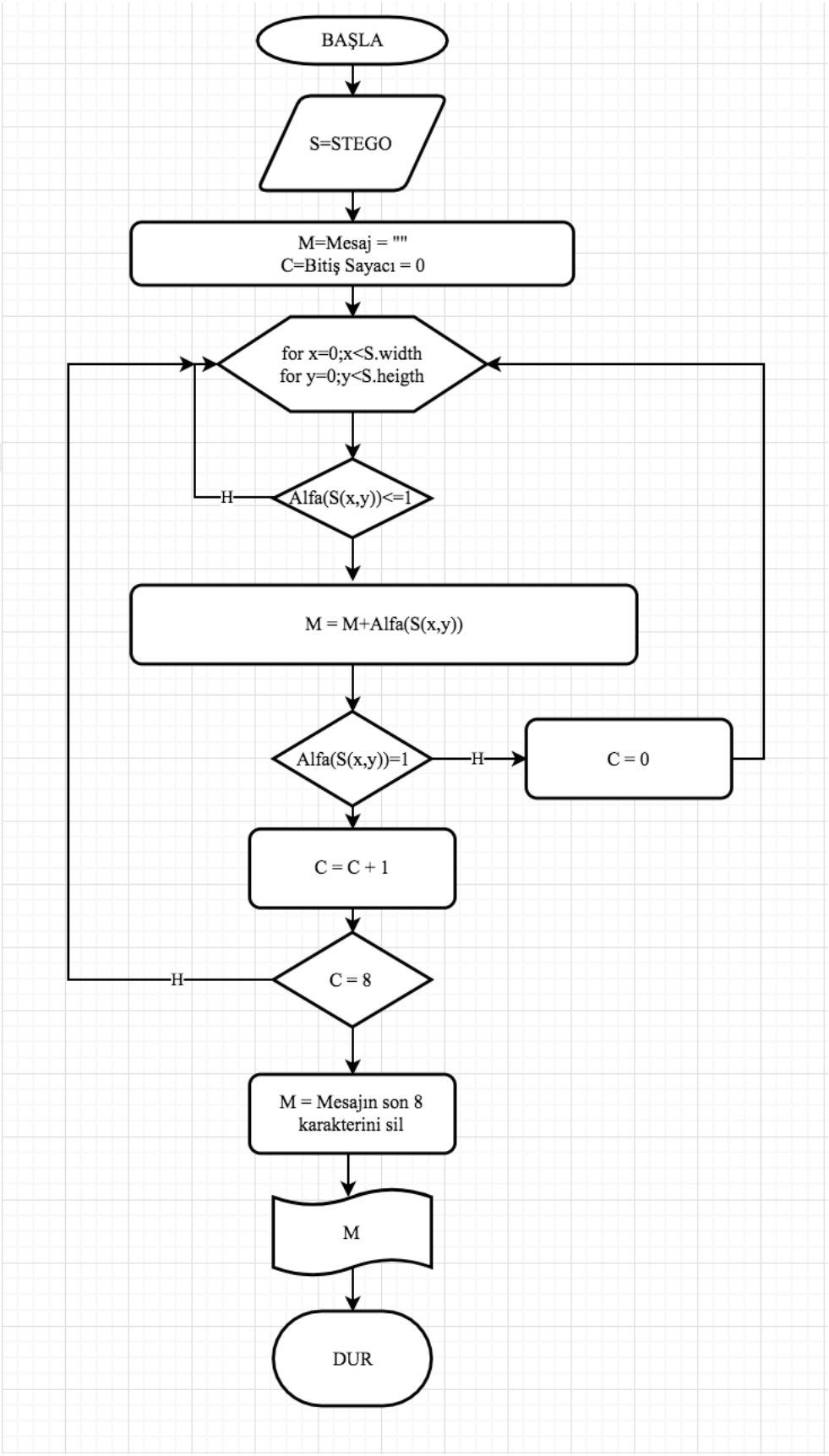
Adım 10:

Mesajı yazdır

Adım 11:

Dur

Şekil 22. Çözme Algoritması



Yeni yaklaşıma ilişkin mesajı Stego nesnesinde saklama ve saklanmış mesajı çözme algoritmaları Şekil 21 ve Şekil 22 de verilmiştir.

Algoritmanın avantajlarından bir tanesi olarak; örneğin 250 harflik bir mesaj saklanılmak istenildiğinde;

$$250 \times 8 + 8 = 2008$$

adet alfa kanalına ihtiyaç duyulmaktadır ki bu değer ile yalnızca ilk 2008 alfa kanalı için değişim olup olmayacağı demektir. Örneğin 768x1024'lük bir resimde 786432 adet alfa değeri olacağı için hesaplanan 2008 değeri ve bu değerlerin yalnızca 1 veya 0'lardan oluşması göz önünde bulundurulmakta olup bu durum insan gözü ile fark edilemeyecek anlamı taşımaktadır.

DÖRDÜNCÜ BÖLÜM

İNCELEME

1. İNCELEME

Yalnızca 0 veya 1 değerlinin yer aldığı alfa kanallarının kullanılması neticesinde, görüntü şeffaflığı üzerinde oluşabilecek değişim, insan gözü ile algılanamamaktadır. Bu durum, resme bakıldığında, bir mesaj içerebileceği hissi uyandırmadığından dolayı Steganografi felsefesine uygun olabilmektedir.

Pikselde yer alan değerler açısından yalnızca alfa kanalının kullanılması ve 0 veya 1 değerlerinin seçilmesi bir kısıt oluşturabilmektedir. Örneğin içinde hiç 0 ve 1 alfa değeri içermeyen görüntülerde bu yaklaşım uygulanamayacağından, resmin bu kriterlere uygun olarak seçilmesi gerekmektedir.

Yeni yaklaşımın kodlandığı uygulama, gönderilmek istenen mesajın dili ve şifrelenmesi açısından ayrıca geliştirilebilir. Bu yaklaşımda, mesajın her harfi için 8 bitlik bir haritalama mevcut olup bilinen harfler ve noktalama bu haritalamaya dahil edilebilmiştir çünkü 8 bit ile 256 karakter kontrol edilebilir. İstenildiğin dinamik olarak bit sayısı arttırılıp azaltılabilir.

Gönderilmek istenen mesajın bittiğini belirten işaret için de haritalamada bir yer ayrılmıştır.

Yaklaşım, yalnızca alfa kanalı destekleyen görüntü formatlarına uygulanabilmektedir ki bu formatlar GIF, PNG, BMP, TIFF, ve JPEG 2000'dir.

SONUÇ

Steganografi biliminde kullanılan tekniklerin güvenilirliği ve kırılması güç algoritmalardan meydana gelmeleri oldukça önemlidir. Aksi durumda gönderilmek istenilen gizli mesajların deşifre olmaları söz konusu olabilmektedir.

Özellikle son yıllarda üretilen kuantum bilgisayarlar ile de şifre kırma çalışmalarında meydana gelen büyük hız ve gelişim, steganografi tekniklerine yeni teknikler bulunması durumunu gerekli kılmıştır. Bu çalışma da steganografi tekniklerine yeni bir yaklaşım getirmeyi amaçlamaktadır.

Çalışmanın getirmek istediği yeni yaklaşım, iki ana başlık üzerinde durmaya çalışmaktadır:

- Görüntü ve kalitesinin bozulmaması
- Kullanılan algoritmanın güvenilirliği

Çalışmada kullanılmak istenen alfa kanalı, görüntünün şeffaflığı ile ilgili olduğu için görüntü üzerinde yer alan renk piksellerini etkilemediğinden bu kanal üzerinde çok daha farklı teknikler geliştirebilmenin mümkün olacağı önerilebilir. Zira bu kanal üzerinde yapılmış başka bir çalışma, Ghaith Salem Sarayreh'in kaleme aldığı tezine de Sayfa 13'de değinilmiştir.

KAYNAKÇA

Ahmed Faleh, **New Method for Image Inside Image Steganography** https://www.researchgate.net/publication/282778985_New_Method_for_Image_Inside_Image_Steganography (erişim tarihi: 28/04/2019)

Anonim, **Justin Bieber - Baby (Reversed)** https://www.youtube.com/watch?v=vgphZB5lzT0 (erişim tarihi: 28/04/2019)

BBC, **WW2 People's War**, https://www.bbc.co.uk/history/ww2peopleswar/stories/59/a3890559.shtml (erişim tarihi:28/04/2019)

Cambridge Üniversitesi, **Digital Watermarking**, https://www.cl.cam.ac.uk/teaching/0910/R08/work/essay-ma485-watermarking.pdf (erişim tarihi:28/04/2019)

Çağdaş Dereli, **Dilbilimsel Steganografi Yöntemleri Üzerine Bir Araştırma** http://acikerisim.ege.edu.tr:8081/jspui/bitstream/11454/4672/1/cagdasdereli2010.pdf (erişim tarihi: 28/04/2019)

Ghaith Salem Sarayreh, **Text Hiding in RGBA Images Using the Alpha Channel and the Indicator Method**,

https://www.meu.edu.jo/uploads/1/5874aeab7257a_1.pdf (erişim tarihi: 28/04/2019)

International Telecommunications Union, **International Morse code**, https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.1677-1-200910-I!!PDF-E.pdf (erişim tarihi:28/04/2019)

Massachusetts Institute of Technology, **Samuel Morse**, https://lemelson.mit.edu/resources/samuel-morse (erişim tarihi:28/04/2019)

Neha Rani ve Jyoti Chaudhary, **Text Steganography Techniques: A Review** http://www.ijettjournal.org/volume-4/issue-7/IJETT-V4I7P186.pdf (erişim tarihi: 28/04/2019)

The National Archives, **Fighting talk: First World War telecommunications**, http://www.nationalarchives.gov.uk/first-world-war/telecommunications-in-war/ (erişim tarihi:28/04/2019)

University College London, **What is Morse Code?**, http://students.cs.ucl.ac.uk/schoolslab/projects/PY2/introduction.html (erişim tarihi:28/04/2019)

University Of Michigan, **Secret methods and Techniques**, http://clements.umich.edu/exhibits/online/spies/methods-ink.html (erişim tarihi:28/04/2019)

Wikizero, **Morse code for non-Latin alphabets**, http://www.wikizero.biz/index.php?q=aHR0cHM6Ly9lbi53aWtpcGVkaWEub3JnL3dpa2kvTW9yc2VfY29kZV9mb3Jfbm9uLUxhdGluX2FscGhhYmV0cw (erişim tarihi:28/04/2019)

ÖZGEÇMİŞ

16 Eylül 1984 tarihi, İzmir ili Bornova ilçesi doğumluyum. İlkokul, ortaokul ve liseyi İzmir'de tamamladıktan sonra 2001 yılında Süleyman Demirel Üniversitesi, Bilgisayar ve Teknoloji Yüksekokulu, Bilgisayar Teknolojisi ve Programlama Meslek Yüksek Okulu'nda önlisans eğitimine kaydoldum. Eğitim tamamlandıktan sonra iş hayatına atıldım. 8 yıl çeşitli şirketlerde çalıştıktan sonra örgün öğretim okuma kararı almam ile birlikte 2010 yılında Dikey Geçiş Sınavına girerek, sınav sonucu doğrultusunda Karadeniz Teknik Üniversitesi, Fen ve Edebiyat Fakültesi, İstatistik ve Bilgisayar Bilimleri bölümün kaydımı gerçekleştirdim. 2013 yılında mezuniyeti sonrasında iş hayatına devam etmem ile birlikte 2016 yılında yüksek lisans kararı aldım ve Beykent Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı'na kaydımı yaptırdım.

Halen, Yapı ve Kredi Bankası A.Ş. , Bankacılık Üssü, Bilgi Teknolojileri Departmanı'nda Uzman BT İş Analisti olarak çalışmaktayım. Evli ve 2 çocuk annesiyim.

Burcu ÜNLÜ