ინფორმაციის დაცვა RGB ფერთა კოდების გამოყენებით

გულნარა კოტრიკაძე, ეკატერინე როჭიკაშვილი,
გიორგი კუჭავა, ანდრო გაფრინდაშვილი, თეიმურაზ მამუკაშვილი
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

შევიმუშავეთ ახალი მეთოდი, სადაც გამოყენებულია სხვადასხვა სიხშირის RGB ფერთა კოდები. მეთოდში გასაღების გამოთვლა ხდება ღია არხით, გასაღები არის ფერი, ინფორმაციაც წარმოდგენილია ფერების სახით, დაშიფრული ინფორმაციაც მიიღება ფერების სახით წარმოდგენილი, რომელიც ეგზავნება მეორე მომხმარებელს, ანუ ფერი არის თავად ინფორმაცია.

საკვანძო სიტყვები: RGB ფერთა კოდები. მედეგობა.

1. შესავალი

კრიპტოგრაფია (წარმოიშვა ბერძნული სიტყვებიდან κρυπτός „კრიპტოს“ — ფარული, და ზმნიდან γράφω „გრაფო“ — წერა, ანუ ფარული წერა) არის მეცნიერება ინფორმაციის დაფარვის შესახებ. კრიპტოგრაფია განიხილება, როგორც მათემატიკისა და კომპიუტერული მეცნიერებების განაყოფი და მჭიდროდ დაკავშირებულია მეცნიერების ისეთ დარგებთან, როგორებიცაა: ინფორმაციის თეორია, კომპიუტერული უსაფრთხოება, ინჟინერინგი და სხვა. დღესდღეობით იგი გამოიყენება ტექნოლოგიურად განვითარებულ სფეროებში, როგორიცაა: საკრედიტო ბარათები, კომპიუტერული პაროლები, ელექტრონული კომერცია და მრავალი სხვა. კრიპტოანალიტიკოსი ინფორმაციის დაშიფვრის გასაღების გამოსათვლელად, მის ხელთ არსებული საწყისი მონაცემებიდან გამომდინარე, ასრულებს ქვემოთ განხილული კრიპტოანალიზური შეტევებიდან ერთ-ერთს:

1. კრიპტოანალიზური შეტევა, როცა ცნობილია მხოლოდ შიფროტექსტი;
2. კრიპტოანალიზური შეტევა, როცა ცნობილია ღია ტექსტი;
3. კრიპტოანალიზური შეტევა, ღია ტექსტის არჩევის შემთხვევაში;
4. კრიპტოანალიზური შეტევა, ღია ტექსტის ადაპტური შერჩევით;
5. კრიპტოანალიზური შეტევა, არჩეული შიფროტექსტის გამოყენებით;
6. კრიპტოანალიზური შეტევა, გასაღებების ყველა შესაძლო ვარიანტების გადარჩევის მეთოდით;
7. ბანდიტური კრიპტოანალიზი (შანტაჟი, წამება, ქრთამი და ა.შ.) [1,3].

2. ინფორმაციის დაცვა საერთო დასაშიფრი ფერის გამოყენებით

პირველ რიგში ანბანის ასო-ნიშნებს, სასვენ ნიშნებს, ციფრებსა და არითმეტიკულ ოპერაციებს მივანიჭოთ სხვადასხვა ფერები, როგორც მონაცემთა ბაზა ჩავწეროთ ცხრილის სახით, რომელიც ცნობილია ყველასათვის, რომლის საშუალებითაც ჩავწერთ საწყის ინფორმაციას ფერების სახით და არა RGB ფორმატით (ცხრილი 1).

ანბანის ასონიშნები, ციფრები, სასვენი ნიშნები და არითმეტიკული ოპერაციები

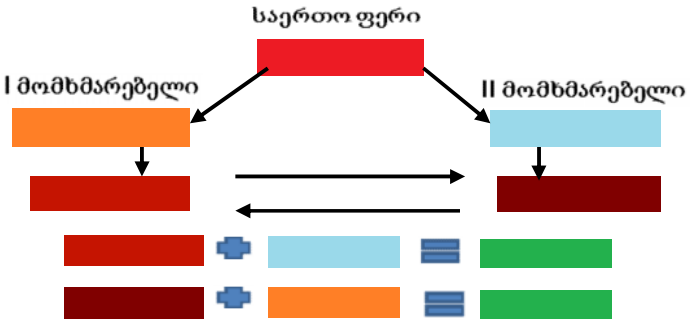
წარმოდგენილია ფერთა სახით (წარმოგენილია ნაწილი). **ცხრ.1**

№	ანბანი	ფერი	კოდი	№	ანბანი	ფერი	კოდი	№	ანბანი	ფერი	კოდი
1	ა		ff0000	4	დ		cccc00	7	ზ		660000
2	ბ		6600ff	5	ე		996600	8	თ		009900
3	გ		00ff99	6	ვ		ffcccc	9	ი		990099

მაგალითად ავიღოთ საწყისი სიტყვა - **„პროგრამა“**:

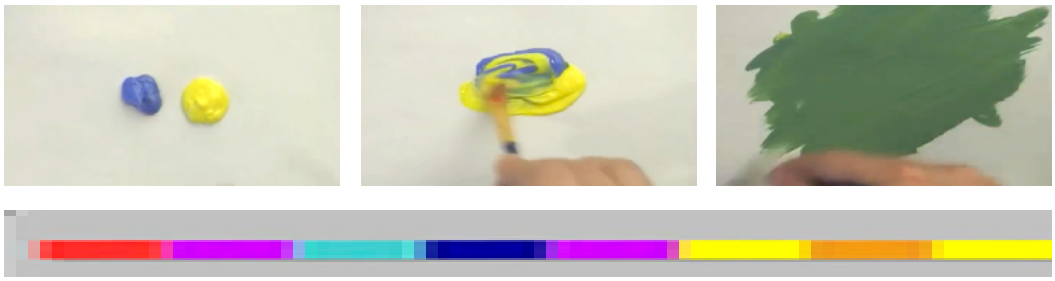
პ	რ	ო	გ	რ	ა	მ	ა

გასაღების მიღების პროცესი: მომხმარებლები საიდუმლოდ ირჩევენ ერთ რომელიმე ფერს, რომელიც გვჭირდება საერთო დასაშიფრი გასაღების მისაღებად, ფერის სახით. ერთ-ერთი მომხმარებელი იღებს თავის საიდუმლო ფერს, საერთო საიდუმლო ფერს უმატებს თავის არჩეულ ფერს და მიიღებს აბსოლუტურად განსხვავებულ შერეულ ფერს და უგზავნის მეორე მომხმარებელს. ანალოგიურად მეორე მომხმარებელიც იღებს თავის შერჩეულ ფერს და უმატებს საერთო საიდუმლო ფერს და მიიღებს შერეულ ფერს. მომხმარებლები ერთმანეთს უგზავნიან შერეულ ფერებს. მიღებულში მომხმარებლები ურევენ კიდევ მათ მიერ აღებულ ფერებს და იღებენ ერთიდაიმავე ფერს, რომელიც არის საერთო დასაშიფრი გასაღები (ნახ.1) [2].



ნახ.1. გასაღების მიღების პროცესი

დაშიფრის ალგორითმი. საწყისი ინფორმაცია წარმოდგენილია ფერების სახით, საერთო დასაშიფრი გასაღებიც მივიღეთ. ახლა განვიხილოთ თუ როგორ უნდა დავშიფროთ ინფორმაცია. დაშიფვრა ხდება შემდეგნაირად: საწყისი ინფორმაციის თითოეულ ფერს ვურევთ მიღებულ საერთო ფერს და ვიღებთ აბსოლუტურად განსხვავებულ ფერთა კომბინაციას და მიღებულ დაშიფრულ ინფორმაციას უგზავნით მეორე მომხმარებელს ღია არხით, ანუ მესამე პირსაც შეუძლია ხელში ჩაიგდოს იგი (ნახ.2).



ნახ.2. ფერთა შერევით მიღებული დაშიფრული საწყისი შეტობინება, სიტყვა „პროგრამა“

ნახ.3. დაშიფრული ინფორმაციის პოზიციების გადანაცვლება

შესაძლებელია გავართულოთ გადასაცემი ფრაზის კოდი. მაგალითად, თითოეული ასონიშნის შესაბამისი ფერი გადავაადგილოთ 7 ადგილით მარჯვნივ (ნახ.3). დაშიფრული შეტყობინება - „პროგრამა განახლდება პირველში ორ საათზე“ [4,5].

დავწეროთ დაშიფრული ტექსტის კოდი: A(i)=K(i)+N, სადაც A(i) წარმოადგენს წასაკითხი ფრაზის ცალკეულ ასოს, გამოსახული შესაბამისი ფერით; K(i) წარმოადგენს გასაღებს (განსახილველ შემთხვევაში მწვანე ფერს); N - წარმოადგენს ბიჯს (განსახილველ შემთხვევაში - 7).

საბოლოო სახით მიღებული დაშიფრული ინფორმაცია (ნახ.3) იგზავნება მეორე კანონიერ მიმხმარებელთან ღია არხით. პირველ რიგში აღნიშნულს შევხედოთ მეორე მომხმარებლის მხრიდან.

მეორე კანონიერი მომხმარებელი გასაშიფრად იქცევა შემდეგნაირად: მიღებული დაშიფრული ინფორმაციის ფერებს გამოაკლებს მათ მიერ მიღებულ საერთო გასაღებს, ანუ მწვანე ფერს და მიიღებს შემდეგ ფერებს (ცხრილი 2).

გაშიფრული ინფორმაცია **ცხრ.2**

პ	რ	ო	გ	რ	ა	მ	ა

მიღებულ ფერთა თანმიმდევრობას შეუსაბამებს საწყის ცხრილში მოცემულ ასონიშნებს და მიიღებს შეტობინებას [4,6].

მესამე პირს რაც შეეხება, მისთვის ცნობილია: 1. წინასწარ შედგენილი ცხრილი, 2. გასაღების გამოთვლის პროცესში ორ-ორი საიდუმლო ფერის შერევით მიღებული ნარევი ფერები, 3. დაშიფრული ინფორმაციის საბოლოო სახე, 4. დაშიფვრის ალგორითმი.

მიუხედავად ამდენი ცნობილი პარამეტრებისა, მესამე პირი მაინც ვერ გაშიფრავს შეტყობინებას, რადგან მისთვის უცნობია საერთო გასაღები, ამ ეტაპზე მწვანე ფერი. თუნდაც რომ ამოიცნოს გასაღების ფერი, უამრავი სხვადასხვა სიხშირის მწვანე ფერი არსებობს. დაშიფრულ ინფორმაციას, მან უნდა გამოაკლოს ის კონკრეტული მწვანე ფერი, რომელიც მომხმარებლებმა გამოიყენეს, ზოგიერთი მწვანე ფერის თექვსმეტობითი კოდი არც გამოაკლდება და თუნდაც გამოაკლდეს, მაინც ვერ მიიღებს ზუსტად იმ სიხშირის ფერს რაც მოცემული გვაქვს ცხრილში, მონაცემთა ბაზის სახით [5].

3. დასკვნა

მიღებული მეთოდის მახასიათებლები: ფერების RGB ფორმატით წარმოდგენა საშუალებას იძლევა გამოყენებულ იქნას 16,5 მილიონი ოდენობის ფერთა გრადაცია. წარმოდგენილ სტატიაში გამოვიყენეთ მხოლოდ 55 ფერი. სხვაობის გამოთვლას აზრი არა აქვს, ფერების იმდენად უზარმაზარი მარაგი არსებობს, ინფორმაციის დაფარვა-გადასაცემად.

ბუნებრივია, დგება საკითხი – როგორია მესამე პირის მიერ გადაცემული ინფორმაციის ხელში ჩაგდების შემთხვევაში მისი გაშიფვრა-ამოკითხვის შანსი ანუ ალბათობა ?

გაშიფვრის ალგორითმი შემდეგნაირია:

1. თითოეული დაშიფრული ასონიშანი წარმოდგენილია ძირითადი და გასაღების ფერის შერევით;

2. K გასაღების სახით მივიღეთ ერთ-ერთი სიხშირის მწვანე ფერი. უამრავი სხვადასხვა სიხშირის მწვანე ფერი არსებობს და ზუსტად იგივე სიხშირის ფერის მიღება, რაც მიიღო მომხმარებლებმა, შეუძლებელია;

3. ნებისმიერი ორი ფერის შერევით ვიღებთ მესამე ფერს, რომელთა გამოჯვნით ისევ საწყის ორ ფერს ვერ მივიღებთ.

ლიტერატურა:

1. Shneier B. Applied Cryptography, John Wiley and Sons. Inc. New York. 1996
2. Application of volumetric matrix in cryptography. Problems of Mechanics. I-ntern. Federation for the Promotion of Mechanism and Machine Science, Tb., 2010
3. Шнайер Б. Прикладная криптография. М., Изд. ТРИУМФ. 2003
4. Андерсон. Джеймс. „Дискретная математика и комбинаторика“. Издательство дом „Вильямс“. 2003г. ;
5. Питерсон У., Уэлдон, Э. Коды, исправляющие ошибки. I-II том. М., „Мир". 1976
6. Касами Т., Токура Н., Ивадари Е., Инагаки Я. Теория кодирования. М., Мир, 1978.

PROTECTION INSFORMATIONS WITH RGB COLOR CODES

Kotrikadze Gulnara, Rodjikashvili Ekaterine,
Kudjava Giorgi, Gaprindashvili Andro, Mamukashvili Teimuraz

Georgian Technical University

Summary

We have developd a new method, which uses a different frequency of RGB color codes. In the Method, the key is calculated whit an open channel, the key is the color, the information are represented as a color, encrypted information which is sent to the customer is presented in the form of colors too, so the color is the information itself.

ЗАЩИТА ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ КОДОВ RGB ЦВЕТОВ

Котрикадзе Г., Рочикашвили Е.,
Кучава Г., Гаприндашвили А., Мамукашвили Т.

Грузинский Технический Университет

Резюме

Разработан новый метод, в котором использованы коды RGB цветов разных частот. В методе, вычисление ключа происходит по открытому каналу. Ключ представляет собой цвет. Информация также представлена в виде цветов. Шифрованная информация, которая пересылается пользователю, представлена также в виде цветов, т.е. цвет представляет саму информацию.